National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme Validation Report

Motorola Solutions, Inc.

Motorola Network Devices S2500, S6000, GGM 8000 with EOS Version 16.0

Report Number: CCEVS-VR-VID10378-2012
Dated: June 30, 2012
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

Acknowledgements

Validation Panel

Dr. Patrick W. Mallett, Lead Scientist

The MITRE Corporation

McLean, VA

Dr. Jerome F. Myers, Senior Engineering Specialist

The Aerospace Corporation

6940 Columbia Gateway Drive, Ste 400

Columbia, MD 21046-2877

Common Criteria Testing Laboratory

Mr. Ryan Day

Mr. Victor Mendoza

Ms. Anne Browne

Mr. Kristopher Kolstad

InfoGard Laboratories, Inc.

San Luis Obispo, CA

Table of Contents

1 Executive Summary

This report documents the Validation Panel's assessment of the CCEVS evaluation of the Motorola Network Devices S2500, S6000, GGM 8000 with EOS version 16.0.

This report is intended to assist the end-user of this product with determining the suitability of this IT product in their environment. End-users should review both the Security Target (ST), which is where specific security claims are made, in conjunction with this Validation Report (VR), which describes how those security claims were evaluated.

The Motorola Network Device models S2500, S6000, and GGM 8000 provide a flexible routing solution for integrated data, voice and virtual private network (VPN) applications.

These solutions feature the Motorola Enterprise OS software suite with a choice of three hardware platforms: S2500/S6000/GGM 8000 series. Each series provides different throughput and scalability capabilities. The common OS software provides Enterprise networking features including: traffic shaping and Quality of Service (QoS), WAN/LAN connectivity, Voice & Multi-Service and Network Management support. Security features provide network and data protection through:

- Firewall Features: Recognizing pre-defined attack types, custom traffic filters.
- Encryption support: The TOE is FIPS 140-2 validated to Level 1 (S2500, S6000) or Level 2 (GGM 8000).
- Secure Tunneling/VPN support: IPsec, FRF.17, and IKE.
- Protocol Authentication: Border Gateway Protocol (BGP), Open Shortest Path First (OSPF), and Protocol Independent Multicast (PIM) protocols.

These network devices feature an Administrative-user interface that allows for the setup, configuration, monitoring and management of the device using a Command Line Interface (CLI) over a local console interface or secured over an SSHv2 secured connection. The TOE also supports encrypted SNMPv3 for a limited set of management functions.

Cryptographic operations provided by the TOE are FIPS 140-2 validated.

The TOE model S2500 and GGM 8000 platforms are suitable for use as edge routers for analog and digital voice systems as well as remote radio frequency (RF) site routers in digital voice systems. Both the S2500 and GGM 8000 may include up to 2 V.24 modules that allow the processing of digital voice, Voice over IP (VoIP). When combined with the analog conventional pluggable module (E&M), the S2500 and GGM 8000 are also suitable as a Conventional Channel Gateway (CCGW) in a Motorola ASTRO® 25 trunked radio communication network. In this role, the TOE exchanges call control traffic via communication with peer devices with ASTRO® 25 controllers.

The E&M pluggable module cannot be used with the S6000 platform.

The S6000 series is suitable as a Wide Area Network (WAN) interface for radio communications network transport systems or as a Core/Edge Network Device.

The S6000 series can also be used to maintain connectivity among small, midsize, and large Local Area networks via a wide variety of WAN services and accommodates virtual port tunneling capabilities with data compression and high speed processing.

When used in the network core, the S6000 supplies high speed, scalable performance for WAN concentration, virtual private network (VPN) tunnel termination, and efficient bandwidth utilization. The S6000 concentrates T1/E1 or T3/E3 internet traffic at the network core, enabling multiple secure tunnels to be maintained through the public network to many remote locations simultaneously.

This table identifies components that must be present in the Operational Environment to support the operation of the TOE.

Component	Description
RADIUS	Authentication Server (optional)[1]
Syslog Host	Syslog host for offloading of audit records
NTP Server	NTP Server
SSHv2 client	SSHv2 client to support Administrative tunnels to the TOE
SNMPv3 Host	Supports SNMPv3 to the net-snmp client on the TOE
Serial Console	Console to perform local administration of the TOE.

Table 1: Operational Environment Components

[1] If your organization requires authentication failure counters and account lockouts for remote accounts, ensure your RADIUS Server supports these features.

2 Identification of the TOE

Table 2 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 organizations and individuals participating in the evaluation.

Evaluation Scheme	United States Common Criteria Evaluation Validation Scheme
Evaluated Target of Evaluation	Motorola Network Devices S2500, S6000, GGM 8000 with EOS version 16.0
Protection Profile	None
Security Target	Motorola Network Devices S2500, S6000, GGM 8000 Security Target EAL 2 augmented ALC_FLR.2
Dates of Evaluation	August 27, 2009 to May 7, 2012
Conformance Result	EAL 2 augmented ALC_FLR.2
Common Criteria Version	Common Criteria for Information Technology Security Evaluation Version 3.1 R3, July 2009
Common Evaluation Methodology (CEM) Version	CEM Version 3.1 R3, July 2009
Evaluation Technical Report (ETR)	11-1757-R-0112 V1.1
Sponsor/Developer	Motorola Solutions, Inc.
Common Criteria Testing Lab (CCTL)	InfoGard Laboratories, Inc.
CCTL Evaluators	Ryan Day, Victor Mendoza, Annie Browne
CCEVS Validators	Rick Murphy, Dr. Patrick Mallett, Dr. Jerome Myers

Table 2: Product Identification

3 Interpretations

The Evaluation Team performed an analysis of the international interpretations of the CC and the CEM and determined that none of the International interpretations issued by the Common Criteria Interpretations Management Board (CCIMB) were applicable to this evaluation.

The TOE is also compliant with all international interpretations with effective dates on or before

August 27, 2009.

4 Security Policy

This section contains the product features and denotes which are within the logical boundaries of the TOE. The following Security Functions are supported by the Motorola Network Device TOE:

- Security Audit
- Identification and Authentication
- User Data Protection: Flow Control
- Cryptographic Operations
- Security Management
- Protection of the TSF

4.1 Security Audit

The Network Device provides an audit capability that generates audit records for administrative-user authentication, configuration and device management sessions and detailed information about traffic management actions taken by the TOE.

The TOE includes separate log categories for System Messaging, User and Configuration Management logs, VPN related logs for IPsec/FRF.17 traffic and Firewall logs that detail packet filtering and actions taken to either permit or deny traffic based on configured attributes.

SNMP traps may also be configured to alert Administrative-users with notification messages for anomalous events or potential security issues as configured by an authorized administrative-user. A series of traps are provided by default, and administrative-users may also customize trap notifications.

Logs are buffered on the TOE and output to a Syslog server in the Operational Environment. The Network Manager and Root roles may access audit logs for review and may delete audit logs within the device buffer. The User role does not have access to audit logs.

4.2 Identification and Authentication

The TOE requires all users to be positively identified and authenticated prior to accessing TSF resources. Administrative-users access the TOE via a local console or SSHv2 (CLI) and SNMPv3. Authentication may be performed by the TOE or a RADIUS server in the Operational Environment.

The TOE maintains three roles by default for CLI access:

- Root (full read/write access)
- Network Manager (full read/write access, except enable/disable of Audit)
- User (read/show current configuration, status)

The TOE maintains two privilege levels for SNMPv3 access:

- MotoAdmin (full read/write access)

- MotoMaster (full read/write access, except for passphrases)

4.3 User Data Protection: Flow Control

The TOE mediates traffic passed through the device, implements packet filtering and enforces configured routing policies as configured by the Network Manager or Root administrative-user.

Flow control rules are enforced through packet filter parameters that explicitly permit or deny traffic flows based on protocol, IP address and connection characteristics that may be indicative of a malicious traffic flow or denial of service attempt. The TOE performs stateful packet inspection based on configured IP addresses and TCP port combinations. This feature allows identification of threats such as Denial of Service (DoS), TCP/IP packet fragmentation attacks, and malicious data injection.

The TOE also supports Internet Key Exchange (IKE) authentication (negotiation) using pre-shared keys as part of FRF.17 and IPsec protocol sessions. IKE negotiation may be initiated in a Data Packet trigger mode or Pre-connect mode.

In support of the Protocol Authentication feature, Protocol Independent Multicast (PIM) authentication support is provided through a manual configuration of cryptographic keys on configured peers. Authentication for BGP and OSPF traffic is provided by the TOE using a shared secret key configured by an authorized administrative-user on peer devices.

4.4 Cryptographic Operations

The TOE is validated as a FIPS 140-2 multi-chip standalone cryptographic module and provides cryptographic support used to encrypt message traffic for IPsec and VPN tunnel sessions, secure connections with peer router devices and establish SSHv2 encrypted sessions. The S2500 andS6000 are FIPS 140-2 Level 1 validated with certificates 1548 and 1547 respectively. The GGM 8000 is FIPS 140-2 Level 2 validated with certificate 1546. The TOE uses 128, 192, and 256 bit AES or 168 bit TDES to encrypt SSHv2, SNMPv3, IPsec, and FRF.17 sessions and 128 bit AES to encrypt persistent keys stored on the TOE.

4.5 Security Management

The Network Device is managed using a CLI and SNMPv3. Administrative-users can perform user management, configuration of routing rules and packet filtering (firewall) options, establish message notifications through SNMP traps and configuration of authentication credentials (key management) to peer devices.

SNMPv3 sessions may also be established with the TOE to provide basic USM user maintenance functions: create, delete, change passphrase, and change security level.

4.6 Protection of TSF

The TOE requires authentication prior to establishing a security association with any device or administrative-user. The TOE is physically secured by the Operational Environment.

TSF data passed during administrative sessions is encrypted to prevent disclosure and is message integrity checked to assure modifications during transit are detected. Trusted channels are established for administrative-user sessions.

TOE services are protected from Denial of Service attacks through quotas placed on TCP connect attempts and for connection-oriented sessions.

Through the enforcement of flow control policies and packet inspection features, potentially malicious data that could affect the TOE or Operational Environment resources may be mitigated based on configuration actions and an audit trail produced allowing detection by administrative-users.

5 TOE Security Environment

5.1 Secure Usage Assumptions

The following assumptions are made about the usage of the TOE:

A.USE	The administrative-user ensures there are no general-purpose computing or storage repository capabilities (e.g., compilers, editors, or user applications) available on the TOE.
A.PHYSICAL	It is assumed that the Operational Environment provides the TOE with appropriate physical security, commensurate with the value of the IT assets protected by the TOE.
A.AVAILABILITY	Network resources shall be available to allow clients to satisfy mission requirements and to transmit information.
A.NTP_SERVER	It is assumed that the Operational Environment provides an NTP server resource for time synchronization purposes for use by the TOE.
A.EAUTH	It is assumed that the Operational Environment provides a RADIUS server resource for remote authentication purposes for use by the TOE if necessary.
A.NOEVIL	The authorized administrative-users are competent; are not careless, willfully negligent, or hostile; and abide by the instructions provided by the TOE documentation.

5.2 Threats Countered by the TOE

The TOE is designed to counter the following threats:

T.AUDIT_COMP	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.AUDACC	Persons may not be accountable for the actions that they conduct because the audit records are not reviewed, thus allowing an attacker to escape detection.
T.TSF_COMP	A malicious user or process may cause TSF data or executable code to be inappropriately accessed (viewed, modified, or deleted).
T.MASQUERADE	A malicious user, process, or external IT entity may masquerade as an authorized entity in order to gain access to data or TOE resources.
T.RESOURCE	A malicious process or user may block others from system resources (e.g., connection state tables, TCP connections) via a resource exhaustion denial of service attack.
T.UNATTENDED	A user may gain unauthorized access to an unattended session.
T.UNAUTH	A user may gain access to user data for which they are not authorized according to the TOE security policy.
T.UNIDENT	The administrative-user may fail to notice potential security violations, thus limiting the administrative-user's ability to identify and take action against a possible security breach.
T.PEER	An unauthorized IT entity may attempt to establish a security association with the TOE.
T.EAVESDROP	A malicious user or process may observe or modify user or TSF data transmitted between physically separated parts of the TOE or a trusted IT Entity.

5.3 Organizational Security Policies

The TOE enforces the following OSPs:

None

6 Architectural Information

The TOE is classified as **Miscellaneous** for Common Criteria purposes. The TOE is made up of *hardware and software* components.

6.1 Architecture Overview

The TOE consists of the Enterprise Operating System Version 16.0 and the S2500, S6000, or GGM 8000 hardware.

6.1.1 TOE Hardware

The following table describes the features of each hardware base unit:

Implementation Characteristics	S2500	GGM 8000	S6000
CPU Internal Operating Frequency	100MHz	1GHz	1GHz
Level-1 Instruction Cache Size / Structure	16KB, 4-Way Set Associative	32KB, 8-Way Set Associative	32KB, 8-Sets (Built-In)
Level-1 Data Cache Size / Structure	8KB, 4-Way Set Associative	32KB, 8-Way Set Associative	32KB, 8-Sets (Built-In)
Level-2 Cache Size	None	512KB	512KB (Built-In)
Cache Coherency on Shared Memory Accesses	No	Yes	Yes
Shared Memory Type	SDRAM	DDR2	SDRAM
Shared Memory Size	32 MB	512 MB	256 MB (DIMM)
Shared Memory Bus Width	32 Bits	64 Bits	64 Bits
Shared Memory Peak Transfer Rate	200 MBS	3,200 MBS	1,064 MBS (133 MTS)
Embedded SW (Flash PROM Memory)	1 MB	32 MB	1 MB
Flash File System (Flash PROM Memory)	16 MB	64 MB	16 MB
Built-In LAN Ports	1 - 10/100	4 – 10/100/1000	3 - 10/100
Built-In WAN Ports	None	2 – T1/E1	None
Pluggable Module Options[2]	Slots for two I/O Modules	Slots for two I/O Modules	Slots for two I/O Modules
Analog CCGW option (4 Port E&M Analog module and DSP module)	Yes	Yes	No

Table 3: Feature comparisons: S2500, S6000 and GGM 8000

[2] Table 4 specifies the maximum number of each module type that each base unit supports.

The hardware platforms allow various configurations using pluggable interface modules to allow the end user to customize the available ports. The following tables illustrate the module combinations that may be used with each platform.

Pluggable Module Combinations by Hardware Platform

Shaded = N/A

Numbers indicate possible configuration options (number of modules supported per chassis)

A single hardware platform device of one of the 3 shown is required for the CC Evaluated configuration.

Module Type/Hardware Platform	S2500 Hardware	GGM 8000 Hardware	S6000 Hardware
T1/E1 (WAN/Telco), 1 port per module	0, 1, 2		
T1/E1 (WAN/Telco), 2 ports per module		0, 1, 2	
T1/E1 (UltraWAN), 4 ports per module			0, 1, 2
T1/E1, 12 ports per module			0, 1, 2
FlexWAN Serial, 1 port per module	0, 1, 2	0, 1, 2	
FlexWAN Serial, 4 ports per module			0, 1, 2
Ethernet 10BASET, 1 port per module	0, 1, 2		
V.24, 2 ports per module	0, 1	0, 1, 2	
T3/E3, 2 ports (one T3/E3) per module			0, 1, 2

Table 4: Pluggable Module Combinations by Hardware Platform

6.1.2 TOE Software

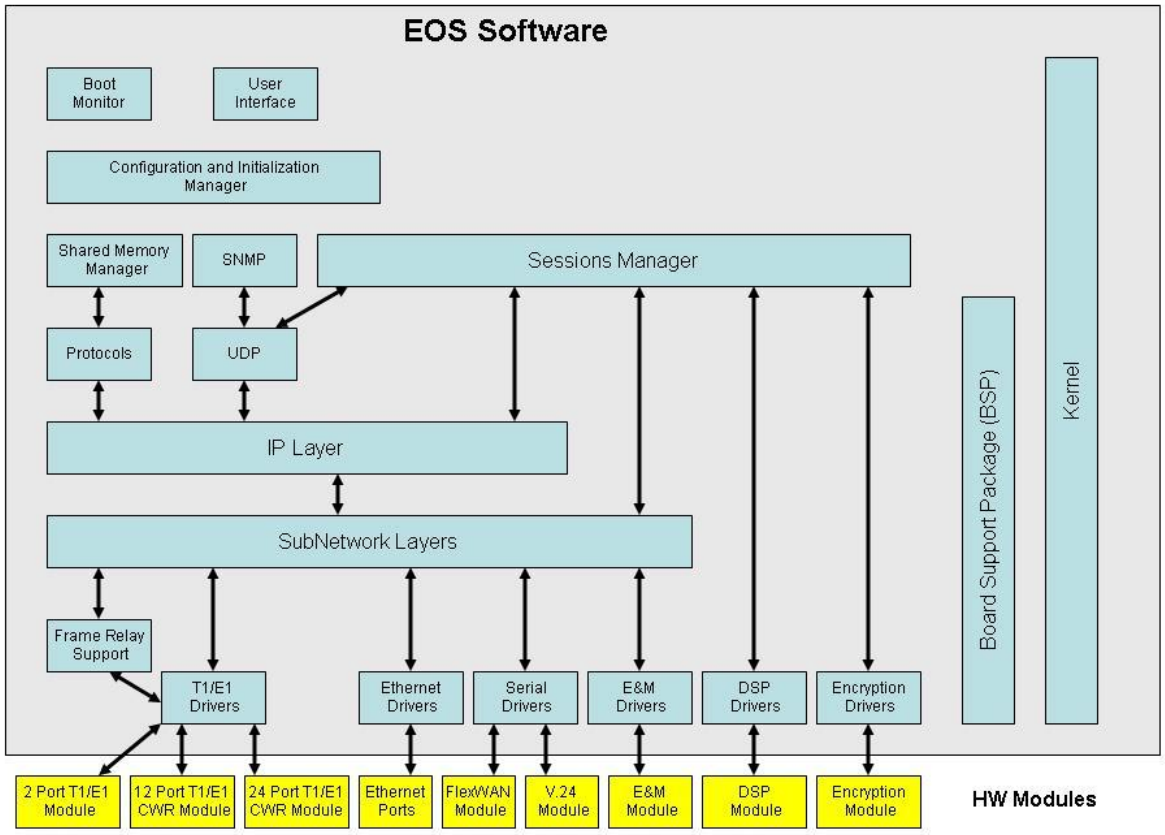

Figure 1: Architecture Overview – Enterprise OS

EOS implements the TOE security functionality. The hardware provides the user with interface and performance options.

7 Clarification of Scope

This section identifies features and components of the marketed product that were not evaluated as part of the TOE. The features were either deemed non-security relevant or are disabled in the evaluated configuration.

7.1 Non-Security Relevant Features

The following features of the TOE relate to network and routing functionality that does not relate to security functions provided by the TOE and are therefore excluded from the evaluation:

- Conventional Channel Gateway (CCGW) deployment aspect
- Cooperative WAN Routing (CWR)

- IP Packet Delay Variation (IPDV)
- SCH Service – Event Schedule features (i.e.: automated backup)
- Bridge service – provides transparent bridging over a variety of LAN and WAN topologies
- Rempolling – Remote Polling Protocol monitors reachability and performance of network devices by polling
- Quality of Service (IPQoS) features
- Load Balancing features
- Performance Management Tools
- Auto startup feature – automatic establishment of PPP and Frame Relay paths upon platform boot
- Distance Vector Multicast Routing Protocol (DVMRP)
- Port Bandwidth Management feature
- Data Compression feature
- Data Prioritization feature
- UDP Broadcast Helper feature
- Diagnostic services
- Integrated Intermediate System to Intermediate System (IISIS) Service – used for IP routing
- IPName Service – determines how names are resolved for Telnet, Ping, and TraceRoute
- IPv6
- Router Discovery Protocol (RDP)
- Routing Information Protocol/Internet Protocol (RIPIP) Service
- Routing Information Protocol Next Generation (RIPNG) Service
- Resource Reservation Protocol (RSVP)
- Spanning Tree Protocol (STP)
- IP-over-IP Tunnel Route Short Cut (TRSC)
- Remote Monitoring (RMON) agent

7.2 Security Relevant Features Excluded from the TOE

The following security relevant features are disabled in the evaluated configuration:

- Telnet access to CLI – only local console and SSHv2 secured sessions are allowed
- SNMPv1 and SNMPv2 – only SNMPv3 is allowed
- Point to Point Tunneling Protocol (PPTP)
- Layer 2 Tunneling Protocol (L2TP)
- Gateway GPRS Support Node (GGSN)
- 2048 bit RSA and DSA key generation and usage

8 Documentation

This section details the documentation that is (a) delivered to the customer, and (b) was used as evidence for the evaluation of the TOE. In these tables, the following conventions are used:

- Documentation that is delivered to the customer is shown with **bold** titles.

- Documentation that was used as evidence but is not delivered is shown in a normal typeface.
- Documentation that is delivered as part of the product but was not used as evaluation is shown with a hashed background.

The TOE is physically delivered to the End-User. The guidance documents are provided for download with the TOE software in accordance with EAL 2 requirements from the Motorola Solutions, Inc. support website and apply to the CC Evaluated configuration:

8.1 Design Documentation

Document	Revision	Date
Motorola Network Devices S2500, S6000, GGM 8000 ADV_FSP.2	0.9	December 1, 2011
Motorola Network Devices S2500, S6000, GGM 8000 ADV_TDS.1	0.4	December 7, 2011
FRF.17 Software Design Specification For EOS	0.4	September 18, 2006
Motorola Network Devices S2500, S6000, GGM 8000 ADV_ARC.1	0.1	January 10, 2011
Request for Comments: 2408, Internet Security Association and Key Management Protocol (ISAKMP)	N/A	November 1998
IPSEC Software Architecture	2.0	December 19, 1997
Frame Relay Privacy Implementation Agreement	N/A	January 21, 2000

8.2 Guidance Documentation

Document	Revision	Date
Motorola Network Device S2500, S6000 and GGM 8000 with EOS Version 16.0 Common Criteria Supplement	0.16	April 19, 2012
Enterprise OS Software Version 16.0 Reference Guide	N/A	January 27, 2011
Enterprise OS Software Version 16.0 User Guide	N/A	January 6, 2011

Document	Revision	Date
Motorola Network Router (MNR) S2500 Hardware User Guide	N/A	March 23, 2011
Motorola Network Router (MNR) S6000 Hardware User Guide	N/A	March 23, 2011
Motorola Transport Gateway GGM 8000 Hardware User Guide	N/A	March 23, 2011

8.3 Configuration Management and Lifecycle

Document	Revision	Date
Motorola Network Devices S2500, S6000, GGM 8000 Configuration Management Plan	0.13	May 3, 2012
Motorola MoCA Software Configuration Management Process	R02.00.00	July 27, 2006
Subscriber Uprev/Change Process	N/A	March 1, 2007
Motorola Network Devices S2500, S6000, GGM 8000 Secure Delivery	0.10	August 3, 2011
Flaw Reporting Procedures, Network Devices S2500, S6000 and TG3500, EAL 2 augmented ALC_FLR.2	0.7	April 25, 2011
Motorola Standard Operating Procedure Part Numbering System	N/A	Oct. 8, 2007
Item Nomenclature Decision Chart	N/A	N/A
WebNIR Process for Infrastructure Planner that uses Schaumburg factory	N/A	2005
Kit, Tanapa, Accessory Group & Allied Model Numbering System and Addenda	N/A	Aug. 1, 2007
GGM 8000 Gateway, MNR S2500, MNR S6000 Common Criteria Tamper Evidence Label Pre-ship Instructions	54009523001-A	May 2011
Motorola GGM 8000, MNR S2500, MNR S6000, FIPS 140-2 Level 2 / Common Criteria Tamper Evidence Label Installation Instructions	54009511001-B	May 2011
Product Flow from Order Entry to Manufacturing	1.0	October 8, 2009

8.4 Test Documentation

Document	Revision	Date
NIAP Security Certification of Motorola Network Transport Gateway Functional Test Plan	4.1	January 27, 2012
Motorola Solutions Network Device ATE_COV.1	0.1	December 5, 2011
Independent and Penetration Test Plan	1.0	May 7, 2012

8.5 Vulnerability Assessment Documentation

Document	Revision	Date
Motorola Network Devices S2500, S6000, GGM 8000 Common Criteria Vulnerability Analysis AVA_VAN.2 EAL2	1.0	December 7, 2011

8.6 Security Target

Document	Revision	Date
Network Devices S2500, S6000, GGM 8000 Security Target EAL2 augmented ALC_FLR.2	1.0	June 13, 2012

9 IT Product Testing

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

9.1 Developer Testing

The test procedures were written by the Developer and designed to be conducted using manual interaction with the TOE interfaces along with test tools to simulate attacks and alerts.

The Developer tested the TOE consistent with the Common Criteria evaluated configuration identified in the ST. The Developer's approach to testing is defined in the TOE Test Plan. The expected and actual test results are also included in the TOE Test Plan. The Developer testing effort tested the available interfaces to the TSF.

The Evaluation Team verified that the Developer's testing tested aspects of the SFRs defined in the ST. This analysis ensures adequate coverage for EAL 2. The Evaluation Team determined that the Developer's actual test results matched the Developer's expected test results.

9.2 Evaluation Team Independent Testing

The Evaluation Team conducted independent testing of the TOE. The Evaluation Team installed the TOE according to vendor installation instructions and the evaluated configuration as identified in the Security Target.

The Evaluation Team confirmed the technical accuracy of the setup and installation guide during installation of the TOE while performing work unit ATE_IND.2-2. The Evaluation Team confirmed that the TOE version delivered for testing was identical to the version identified in the ST.

The Evaluation Team used the Developer's Test Plan as a basis for creating the Independent Test Plan. The Evaluation Team analyzed the Developer's test procedures to determine their relevance and adequacy to test the security function under test. The following items represent a subset of the factors considered in selecting the functional tests to be conducted:

- Security functions not extensively tested by the developer's tests
- Security functions that implement critical security features
- Security functions critical to the TOE's security objectives
- Security functions with open parameters (e.g. text fields, unbounded number fields)

Each TOE Security Function was exercised at least once and the Evaluation Team verified that each test passed.

9.3 Vulnerability Analysis

The Evaluation Team ensured that the TOE does not contain exploitable flaws or weaknesses in the TOE based upon the Evaluation Team's vulnerability analysis and penetration tests.

The Evaluators performed a vulnerability analysis of the TOE to identify any obvious vulnerabilities in the product and to determine if they are exploitable in the intended environment for the TOE operation. In addition, the Evaluation Team performed a public domain search for potential vulnerabilities. The public domain search did not identify any known vulnerabilities in the TOE as a whole or any components of the TOE.

Based on the results of the Evaluation Team's vulnerability analysis, the Evaluation Team devised penetration testing to confirm that the TOE was resistant to penetration attacks performed by an attacker with Basic attack potential. The Evaluation Team conducted testing using the same test configuration that was used for the independent testing. In addition to the documentation review used in the independent testing, the team used the knowledge gained during independent testing and the design activity to devise the penetration tests. The penetration tests attempted to misuse components of the TOE and put the TOE in undefined states. This resulted in a set of four penetration tests.

10 Results of the Evaluation

The evaluation was carried out in accordance with the Common Criteria Evaluation and Validation Scheme (CCEVS) processes and procedures. The TOE was evaluated against the

criteria contained in the Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 3. The evaluation methodology used by the Evaluation Team to conduct the evaluation is the Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 3.

InfoGard has determined that the TOE meets the security criteria in the Security Target, which specifies an assurance level of EAL 2 + ALC_FLR.2. A team of Validators, on behalf of the CCEVS Validation Body, monitored the evaluation. The evaluation was completed on June 30, 2012.

11 Validator Comments/Recommendations

The TOE only provides internal storage for 64 KB of audit records. Audit records will be overwritten if the TOE's internal audit storage is exceeded during operation. Potential customers are advised that steps need to be taken to monitor the audit storage on the TOE and take preventative action to move audit data to auxiliary storage into the respective operational environment before any audit records are lost due to being overwritten.

This evaluation started at time when compliance with a Protection Profile (PP) was expected if one was available. This product is close to a PP, but the main features that were of customer interest were packet radio network capabilities that do not fit any PP. Hence, the TOE was not evaluated and validated against a PP. The CCTL presented an analysis that the TOE could not meet existing profiles, such as Router, Firewall, or VPN PPs. The analysis was reviewed by CCEVS, who decided to permit the evaluation to proceed.

The protocol, IPv6 was excluded from the evaluation.

12 Security Target

Motorola Network Devices S2500, S6000, GGM 8000 Security Target EAL2 augmented ALC_FLR.2, Version 1.0, June 13, 2012.

13 Terms

13.1 Acronyms

CC	Common Criteria
CSP	Critical Security Parameters
DAC	Discretionary Access Control
EAL	Evaluation Assurance Level
FIPS	Federal Information Processing Standards Publication 140-2
IDS	Intrusion Detection System
IPS	Intrusion Prevention System
I/O	Input/Output
MIB	Management Information Base

NIST	National Institute of Standards and Technology
OCSP	Online Certificate Status Protocol
PP	Protection Profile
SF	Security Functions
SFR	Security Functional Requirements
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functions

13.2 Terminology

Administrative-users	Refers to a TOE account holder for the purpose of performing Administrative duties including the following roles: (CLI roles) Root, Network Manager, User; (SNMPv3 roles) MotoAdmin, MotoMaster.
Base Unit	The gateway or router without any interface modules installed.
Conventional Channel Gateway	Refers to a TOE feature applicable to the S2500 and GGM 8000 platform where the TOE provides an analog or digital voice interface and control functions for a conventional voice network
Critical Security Parameter	Security-related information (e.g., secret and private cryptographic keys, and authentication data such as passwords and PINs) whose disclosure or modification can compromise the security of a cryptographic module.
Key Encryption Key (KEK)	The master key that encrypts persistent critical security parameters (CSPs) such as keys, secrets, and passwords.
IKE Pre-Shared Keys	Used to authenticate peer to peer during IKE session
FRF.17	(Frame Relay Forum) Frame Relay Privacy Implementation Agreement
Network Management Console	Refers to the IT Entity used by an authorized administrative-user to communicate via CLI or SNMPv3 with the TOE for TSF management.
User Security Model	Provides authentication and privacy (encryption) functions and operates at the message level. (SNMPv3)
View based access control model	Determines whether a given principal is allowed to access

a particular MIB object to perform specific functions and operates at the protocol data unit (PDU) level.

14 Bibliography

[1] Common Criteria for Information Technology Security Evaluation – Part 1: Introduction and general model, dated July 2009, Version 3.1 Revision 3, CCMB-2009-07-001.

[2] Common Criteria (CC) for Information Technology Security Evaluation – Part 2: Security functional components, July 2009, Version 3.1, Revision 3, CCMB-2009-07-002.

[3] Common Criteria for Information Technology Security Evaluation – Part 3: Security assurance components, July 2009, Version 3.1, Revision 3, CCMB-2009-07-003.

[4] Common Methodology for Information Technology Security Evaluation – Evaluation methodology, July 2009, Version 3.1, Revision 3, CCMB-2009-07-004.