Haivision Makito 2.1 Security Target

for Common Criteria Version 3.1, Revision 3

<table>
<tr><td>Document Type</td><td colspan="2">Document Number</td><td>Version</td><td>Status</td></tr>
<tr><td>Security Target</td><td colspan="2"><b>HVS-PD-ST-MAK211</b></td><td>1.1</td><td>Released</td></tr>
<tr><td colspan="2">Created</td><td colspan="3">Last Updated</td></tr>
<tr><td colspan="2">09 September 2011</td><td colspan="3">29 May 2013</td></tr>
<tr><td colspan="2">Author</td><td colspan="3">Title</td></tr>
<tr><td colspan="2">Jean Dubé
John Linton
Steve Matthews</td><td colspan="3">Sr. Embedded Systems Developer
Product Manager
Manager, Technical & QMS Documentation</td></tr>
<tr><td colspan="5"></td></tr>
</table>

Copyright © 2012 Haivision Network Video. All rights reserved. The Haivision logo, Furnace, Mako, Makito, Barracuda, Piranha, Stingray, InStream, Torpedo and CoolSign are trademarks of Haivision Network Video. Other trademarks identified in this document are the property of their respective owners. All specifications are subject to change without notice.

Table of Contents

Copyright © 2012 Haivision Network Video. All rights reserved. The Haivision logo, Furnace, Mako, Makito, Barracuda, Piranha, Stingray, InStream, Torpedo, Kraken, CoolSign, KulaByte and Hydra are trademarks of Haivision Network Video. Other trademarks in this document are the property of their respective owners. All specifications are subject to change without notice.

Copyright © 2012 Haivision Network Video. All rights reserved. The Haivision logo, Furnace, Mako, Makito, Barracuda, Piranha, Stingray, InStream, Torpedo, Kraken, CoolSign, KulaByte and Hydra are trademarks of Haivision Network Video. Other trademarks in this document are the property of their respective owners. All specifications are subject to change without notice.

Copyright © 2012 Haivision Network Video. All rights reserved. The Haivision logo, Furnace, Mako, Makito, Barracuda, Piranha, Stingray, InStream, Torpedo, Kraken, CoolSign, KulaByte and Hydra are trademarks of Haivision Network Video. Other trademarks in this document are the property of their respective owners. All specifications are subject to change without notice.

Preface

Haivision Systems Inc. (d/b/a “Haivision” or “Haivision Network Video”) is the global leader in delivering the most advanced video networking, digital signage, and IP video distribution solutions. Haivision is the only company that offers complete end-to-end technology for video, graphics, and metadata in this field and makes this technology available as solutions through integrators and resellers worldwide. Haivision has specific expertise in the education, medical, government/military, enterprise/retail, and sports/entertainment markets.

Haivision is based in Montreal and Chicago, serving global markets via channel partners, systems integrators, and OEM partners. Haivision was the first company to develop advanced, high performance, and low latency H.264 codec technology. Since early 2009, we have been shipping our 4th generation H.264 implementation supporting high definition up to 1080p60. Today, we are viewed as the undisputed leader in performance IP Video delivery.

Haivision Systems Inc.
4445 Garand,
Montreal, Quebec
Canada H4R 2H9

Customers, or other interested parties, are encouraged to visit our Website for additional information or to provide feedback on our products.

www.haivision.com

Copyright © 2012 Haivision Network Video. All rights reserved. The Haivision logo, Furnace, Mako, Makito, Barracuda, Piranha, Stingray, InStream, Torpedo, Kraken, CoolSign, KulaByte and Hydra are trademarks of Haivision Network Video. Other trademarks in this document are the property of their respective owners. All specifications are subject to change without notice.

Document Introduction

1.1 Conventions

Security Functional Requirements, Part 2 of the CC, defines an approved set of operations that may be applied to functional requirements: *refinement*, *assignment*, *selection*, and *iteration*. The following conventions have been applied in this document:

1. The **assignment** operation is used to assign a specific value to an unspecified parameter, such as the length of a password. Assignment is indicated by showing the value in red text inside square brackets, [assignment value].
2. The **selection** operation is used to select one or more options provided by the CC in stating a requirement. Selections are denoted by italicized red text inside square brackets, [*selection value*].
3. The **iteration** operation is used when a component is repeated with various operations. Iteration is denoted by showing the iteration number in red text inside parenthesis (iteration number) following the component identifier.
4. The **refinement** operation is used to add detail to a requirement, and thus further restricts a requirement.

   Refinement of additional security requirements is denoted by **bold underline text** in red.

1.2 Terminology

Term	Definition
A/V	Audio/Video
AES	Advanced Encryption Standard
ASE	Evaluation Assurance Class: Security Target Evaluation
AVS	Algorithm Validation System
bps	Bits per second
BNC	Bayonet Neill–Concelman; coaxial cable quick connect/disconnect RF connector
CA	Certificate Authority
CAVP	Cryptographic Algorithm Validation Program
CBC	Cipher Block Chaining
CC	Common Criteria
CFB	Cipher Feedback

Copyright © 2012 Haivision Network Video. All rights reserved. The Haivision logo, Furnace, Mako, Makito, Barracuda, Piranha, Stingray, InStream, Torpedo, Kraken, CoolSign, KulaByte and Hydra are trademarks of Haivision Network Video. Other trademarks in this document are the property of their respective owners. All specifications are subject to change without notice.

Term	Definition
CIF	Common Intermediate Format
CLI	Command Line Interface
CMVP	Cryptographic Module Validation Program
CSP	Critical Security Parameter
CSR	Certificate Signing Request
DH	Diffie-Hellman
DNS	Domain Name System
DRBG	Deterministic Random Bit Generator
DSA	Digital Signature Algorithm
DVI	Digital Video Interface
EAL	Evaluation Assurance Level
FIPS	Federal Information Processing Standard
FIPS Pub	Federal Information Processing Standards Publication
FPGA	Field Programmable Gate Array
GOP	Group of Pictures
GUI	Graphical User Interface
HD	High-Definition
HD-SDI	High Definition Serial Digital Interface
HMAC	Hash-based Message Authentication Code
HTTPS	Hypertext Transfer Protocol Secure (HTTPS) is a combination of the Hypertext Transfer Protocol with the SSL/TLS protocol to provide encryption and secure identification of the server.
Hz	Hertz
IP	Internet Protocol. An Internet Protocol (IP) address is a numerical label that is assigned to devices participating in a computer network that uses the Internet Protocol for communication
IPTV	Internet Protocol Television
IT	Information Technology

Copyright © 2012 Haivision Network Video. All rights reserved. The Haivision logo, Furnace, Mako, Makito, Barracuda, Piranha, Stingray, InStream, Torpedo, Kraken, CoolSign, KulaByte and Hydra are trademarks of Haivision Network Video. Other trademarks in this document are the property of their respective owners. All specifications are subject to change without notice.

Term	Definition
KAT	Known Answer Test
KLV	Key-Length-Value
LAN	Local Area Network
LSB	Least Significant Bit
MPEG	Moving Picture Experts Group
NDPP	Network Device Protection Profile
NIST	National Institute of Standards and Technology
NTP	Network Time Protocol (a protocol used to synchronize the clocks of computers to sometime reference)
OSP	Organization Security Policy
PAM	Pluggable Authentication Modules
PBKDF2	Password-Based Key Derivation Function 2
PP	Protection Profile
PRBS	Pseudo Random Binary Sequencer
RFC	Request for Comments (Internet Engineering Task Force)
RGB	Red Green Blue (color model)
RNG	Random Number Generator
RSA	A security firm (division of EMC Corp.) and encryption algorithm
RTP	Real-time Transport Protocol
RTMP	Real-Time Messaging Protocol
RTSP	Real Time Streaming Protocol
SAR	Security Assurance Requirements
SD	Standard Definition
SD-SDI	Standard Definition Serial Digital Interface
SFR	Security Functional Requirements
SHA	Secure Hash Algorithm
SNMP	Simple Network Management Protocol

Copyright © 2012 Haivision Network Video. All rights reserved. The Haivision logo, Furnace, Mako, Makito, Barracuda, Piranha, Stingray, InStream, Torpedo, Kraken, CoolSign, KulaByte and Hydra are trademarks of Haivision Network Video. Other trademarks in this document are the property of their respective owners. All specifications are subject to change without notice.

Term	Definition
SP	Special Publication (NIST)
SSH	Secure Shell
SSL	Secure Socket Layer (also known as TLS). SSL are cryptographic protocols that provide security for communications over networks such as the Internet
ST	Security Target
TLS	Transport Layer Security
TOE	Target of Evaluation
TS-MPEG	MPEG Transport Stream
TSF	TOE Security Function
TSS	TOE Summary Specification
URL	Uniform Resource Locator; the best-known example of a URL is the address of a web page on the World Wide Web
VLC	Open source media player and multimedia framework
WAN	Wide Area Network
WCI	Web-based Customer Interaction

1.3 References

- Protection Profile: Security Requirements for Network Devices, Information Assurance Directorate, 8 Jun 2012, Version 1.1
- Common Criteria for Information Technology Security Evaluation Part 1: Introduction and general model, Jul 2009, Version 3.1 Revision 3 Final, CCMB-2009-07-001
- Common Criteria for Information Technology Security Evaluation Part 2: Security functional components, Jul 2009, Version 3.1 Revision 3 Final, CCMB-2009 -07-002
- Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components, Jul 2009, Version 3.1 Revision 3 Final, CCMB-2009 -07-003
- Common Methodology for Information Technology Security Evaluation (CEM), Jul 2009, Version 3.1 Revision 3 Final, CCMB-2009 -07-004
- FIPS 140-2, May 2001, Security Requirements for Cryptographic Modules

Copyright © 2012 Haivision Network Video. All rights reserved. The Haivision logo, Furnace, Mako, Makito, Barracuda, Piranha, Stingray, InStream, Torpedo, Kraken, CoolSign, KulaByte and Hydra are trademarks of Haivision Network Video. Other trademarks in this document are the property of their respective owners. All specifications are subject to change without notice.

- NIST Implementation Guidance for FIPS Pub 140-2 and the Cryptographic Module Validation Program, Jul 2011
- FIPS 180-3, Oct 2008, Secure Hash Standard (SHS)
- FIPS 186-2, Jan 2000, Digital Signature Standard (DSS)
- FIPS 186-3, Jun 2009, Digital Signature Standard (DSS)
- FIPS 197, Nov 2001, Advanced Encryption Standard
- FIPS 198-1, Jul 2008, The Keyed-Hash Message Authentication Code (HMAC)
- NIST SP 800-38 A, Dec 2001, Recommendation for Block Cipher Modes of Operation - Methods and Techniques
- NIST SP 800-56 B, Aug 2009, Recommendation for Pair-Wise Key Establishment Schemes Using Integer Factorization Cryptography
- NIST SP 800-90, Mar 2007, Recommendation for Random Number Generation Using Deterministic Random Bit Generators
- OpenSSL FIPS 140-2 Security Policy, Version 2.0.1, Jul 2012
- PKCS#1 v2.1 Jun 2002 RSA Cryptography Standard
- RFC 2246, The TLS Protocol, Version 1.0, Jan 1999
- RFC 2346, Making Postscript and PDF International, May 1998
- RFC 2818, HTTP Over TLS, May 2000
- RFC 4251, The Secure Shell (SSH) Protocol Architecture, Jan 2006
- RFC 4252, The Secure Shell (SSH) Authentication Protocol, Jan 2006
- RFC 4253, The Secure Shell (SSH) Transport Layer Protocol, Jan 2006
- RFC 4254, The Secure Shell (SSH) Connection Protocol, Jan 2006
- RFC 4255, Using DNS to Securely Publish Secure Shell (SSH) Key Fingerprints, Jan 2006
- RFC 4346, The Transport Layer Security (TLS) Protocol, Version 1.1, Apr 2006
- RFC 5246 The Transport Layer Security (TLS) Protocol, Version 1.2, Aug 2008

1.4 Document Organization

Section 1 – Introduction: provides ST and TOE references, conformance claims, an overview of the TOE, and a description of its physical and logical scope.

Section 2 – Security Problem Definition: details the expectations for the TOE environment, including the assumptions, organizational security policies, and threats that are countered by the TOE and its environment.

Section 3 – Security Objectives: details the security objectives of the TOE and its Operational Environment.

Copyright © 2012 Haivision Network Video. All rights reserved. The Haivision logo, Furnace, Mako, Makito, Barracuda, Piranha, Stingray, InStream, Torpedo, Kraken, CoolSign, KulaByte and Hydra are trademarks of Haivision Network Video. Other trademarks in this document are the property of their respective owners. All specifications are subject to change without notice.

Section 4 – Security Requirements: details the security functional requirements (SFRs) for the TOE, and the Security Assurance Requirements as per the applicable Protection Profile.

Section 5 – TOE Summary Specification: describes the security functions represented in the TOE that satisfy the security requirements.

Section 6 – Security Requirements Rationale: demonstrates the completeness and sufficiency of SFRs that fulfill the objectives of the TOE and shows that the SFR and SAR dependencies are satisfied.

1.5 Document History

Version	Status	Description of Changes	YYYY/MM/DD	Changed by:
1.1	Released	• First public issue	2013/05/29	S. Matthews

Copyright © 2012 Haivision Network Video. All rights reserved. The Haivision logo, Furnace, Mako, Makito, Barracuda, Piranha, Stingray, InStream, Torpedo, Kraken, CoolSign, KulaByte and Hydra are trademarks of Haivision Network Video. Other trademarks in this document are the property of their respective owners. All specifications are subject to change without notice.

2. Introduction (ASE_INT)

2.1 ST and TOE Reference

ST Title	Haivision Makito 2.1.1 Security Target
ST Document Number	HVS-PD-ST-MAK211
ST Version	Version 1.1
ST Issue Date	29 May 2013
TOE Identification	Blades: B-290E-DVI, B-290E-DVI-S, B-290E-HDSDI, B-280E-SDI Firmware Option: SW-290E-KLV Chassis: F-280-1, F-290-1, F-290-1DH, F-MB6B-RAC, F-MB6X-RAC, F-MB6B-DC, F-MB6B-MED, F-MB21B-R Appliances: S-290E-AIR, S-290E-DVI, S-290E-HDSDI, S-280E-SDI TOE hardware variants must have firmware version 2.1.1-3.
TOE Developer	Haivision Systems Inc.
CC Identification	CC Version 3.1 Revision 3
Protection Profile	Security Requirements for Network Devices, Version 1.1
ST Author	Jean Dubé
Keyword	Makito

Table 1: ST and TOE Reference

2.2 TOE Overview

The TOE is a full-featured, high-performance IP audio/video encoder that is capable of encoding H.264 video at resolutions of up to 1080p60, with a latency of less than 55 milliseconds. The TOE can also support computer display input at resolutions up to 1920x1080@60 Hz or 1280x1024@75 Hz.

The TOE can take any one of several forms, based on a combination of blades, firmware options, and chassis/appliances described in the tables below. Please note the following:

- Each blade is identical except for the number and type of physical interfaces.

Copyright © 2012 Haivision Network Video. All rights reserved. The Haivision logo, Furnace, Mako, Makito, Barracuda, Piranha, Stingray, InStream, Torpedo, Kraken, CoolSign, KulaByte and Hydra are trademarks of Haivision Network Video. Other trademarks in this document are the property of their respective owners. All specifications are subject to change without notice.

- The KLV firmware option refers to non-TSF related functionality (factory installed).
- Firmware version is 2.1.1-3.
- Chassis serve only to enclose the blades and to provide power distribution.
- Appliances are a combination of one blade in a single-slot enclosure.

Product Reference #	Description
Blades	
B-290E-DVI	Makito HD-DVI H.264 Encoder blade
B-290E-DVI-S	Makito HD-DVI H.264 Encoder blade with serial port
B-290E-HDSDI	Makito HD-SDI H.264 Encoder blade
B-280E-SDI	Barracuda SD-SDI H.264 Encoder blade
Firmware Options	
SW-290E-KLV	KLV metadata support, a licensable feature providing Key Length Value encoding functionality (see section 1.3.2.3)
FCO-SV-SW-CONFIG	A specific firmware version can be requested by including this part number in the purchase order. Please specify the 2.1.1-3 release as part of the configuration information in order to receive the firmware described in this Security Target.
Chassis	
F-280-1	Single-slot Barracuda enclosure with AC power supply
F-290-1DH	Dual height, single-slot Makito enclosure with AC power supply
F-290-1	Single-slot Makito enclosure with AC power supply
F-MB6B-RAC	Second generation 6-slot chassis with redundant AC power supply (can hold any B- blade)
F-MB6X-RAC	Same as F-MB6B-RAC, but with new power supplies for MakitoX series (can hold any B- blade)
F-MB6B-DC	Second generation 6-slot chassis with DC power supply (can hold any B- blade)

Copyright © 2012 Haivision Network Video. All rights reserved. The Haivision logo, Furnace, Mako, Makito, Barracuda, Piranha, Stingray, InStream, Torpedo, Kraken, CoolSign, KulaByte and Hydra are trademarks of Haivision Network Video. Other trademarks in this document are the property of their respective owners. All specifications are subject to change without notice.

Product Reference #	Description
F-MB6B-MED	Second generation 6-slot chassis with medical-grade AC power supply (can hold any B- blade)
F-MB21B-R	Second generation 21-slot chassis with redundant power supplies (can hold any B- blade)
Appliances	
S-280E-SDI	Barracuda SD-SDI H.264 Encoder appliance (B-280E-SDI) in single-card enclosure (F-280-1)
S-290E-HDSDI	Makito HD-SDI H.264 Encoder appliance (B-290E-HDSDI) in single-card enclosure (F-290-1)
S-290E-DVI	Makito HD-DVI H.264 Encoder appliance (B-290E-DVI) in single-card enclosure (F-290-1)
S-290E-DVI-S	Makito HD-DVI H.264 Encoder appliance (B-290E-DVI-S) in single-card, dual-height enclosure (F-290-1DH)
S-290E-AIR	Makito Air Ruggedized HD/SD H.264 Video Encoder with SW-290E-KLV

Table 2: TOE Product Reference Numbers

A customer that orders a product (or combination of products) from the table above must also indicate that the order should include FCO-SV-SW-CONFIG, specifying firmware version 2.1.1-3. This is to ensure that the products ordered will correspond to the TOE described by this Security Target.

The differences in the blades include the number of ports, interfaces, and throughput. Although these blades have different specifications (in terms of performance and capabilities), they all provide the same security functions described in the ST. They are therefore considered to be the same for the purposes of the ST description. The variants of the TOE hardware are described in the table below:

Appliance	Blade	Card Type	Hardware Version[1]	Video IN	HD	Serial Port	Slot Height	KLV
S-280E-SDI	B-280E-SDI	Barracuda Encoder Gen-II	--	BNC		√	1	Option
S-290E-HDSDI	B-290E-HDSDI	Makito-SDI Encoder Gen-II	--	BNC	√	√	1	Option
S-290E-DVI	B-290E-DVI	Makito-DVI Encoder	B-	DVI-I	√		1	Option

[1] A hardware version of '--' (pronounced dash dash) represents the first release of the hardware.

Copyright © 2012 Haivision Network Video. All rights reserved. The Haivision logo, Furnace, Mako, Makito, Barracuda, Piranha, Stingray, InStream, Torpedo, Kraken, CoolSign, KulaByte and Hydra are trademarks of Haivision Network Video. Other trademarks in this document are the property of their respective owners. All specifications are subject to change without notice.

Appliance	Blade	Card Type	Hardware Version[1]	Video IN	HD	Serial Port	Slot Height	KLV
S-290E-DVI-S	B-290E-DVI-S	Makito-DVI Encoder	B-	DVI-I	√	√	2	Option
S-290E-AIR[2]		Makito-SDI Encoder Gen-II	--	BNC	√	√	N/A	Yes

Table 3: TOE Hardware Variants

There is no difference between the products and the TOE. The physical boundary of each product that comprises the TOE is the enclosure.

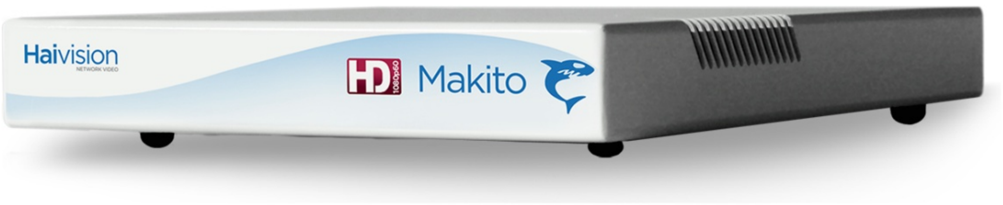


Figure 1: Enclosure for Makito HD-DVI and Makito HD-SDI encoders (F-290-1)

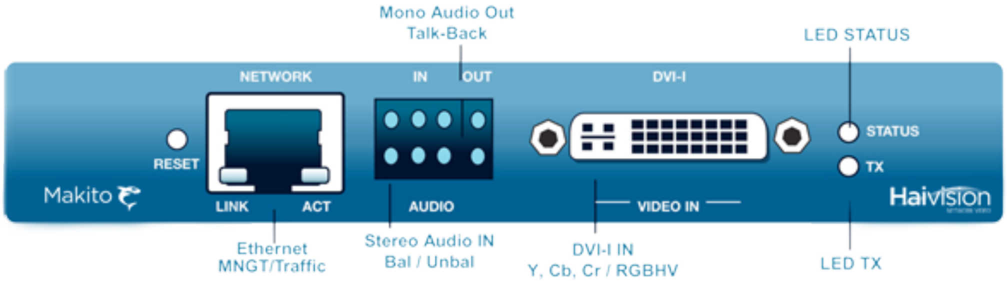


Figure 2: Rear panel of the Makito HD-DVI encoder (B-290E-DVI)

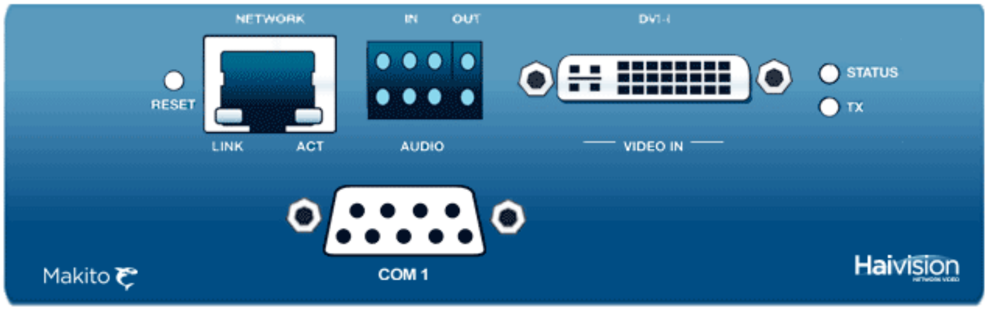


Figure 3: Rear panel of the dual-height Makito HD-DVI encoder (B-290E-DVI-S)

[2] The blade contained in this ruggedized appliance is not sold separately.

Copyright © 2012 Haivision Network Video. All rights reserved. The Haivision logo, Furnace, Mako, Makito, Barracuda, Piranha, Stingray, InStream, Torpedo, Kraken, CoolSign, KulaByte and Hydra are trademarks of Haivision Network Video. Other trademarks in this document are the property of their respective owners. All specifications are subject to change without notice.

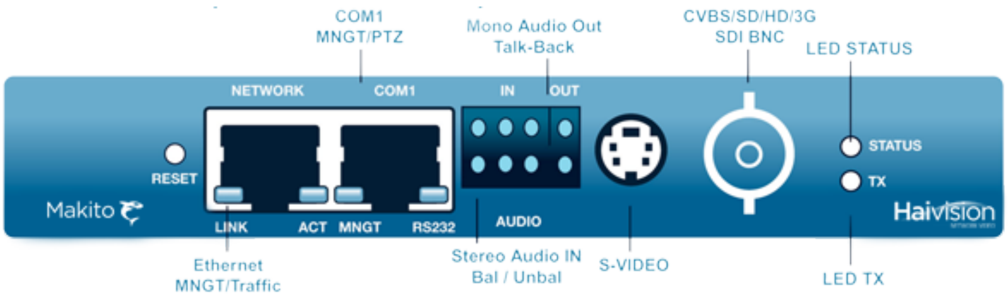


Figure 4: Rear panel of the Makito HD-SDI encoder (B-290E-HDSDI)

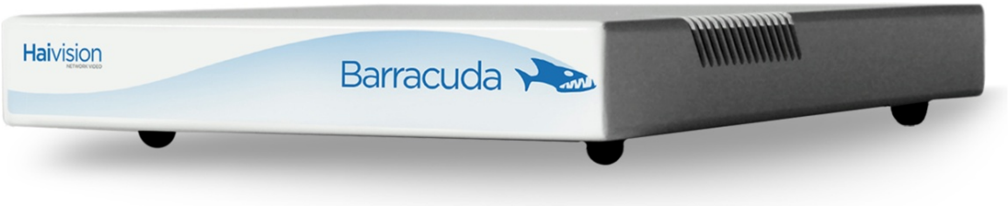


Figure 5: Enclosure for Barracuda SD-SDI encoder (F-280-1)

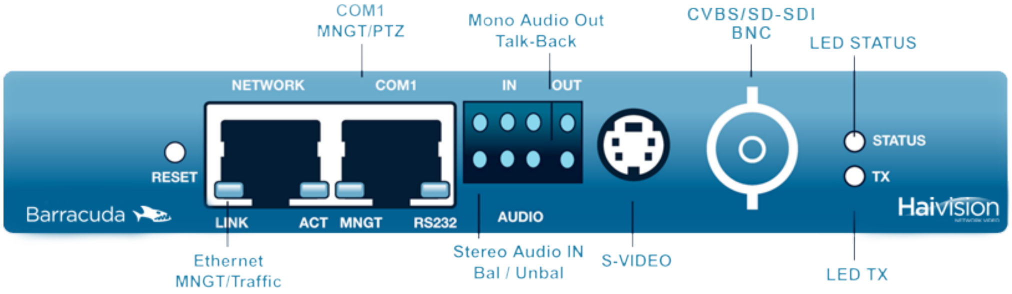


Figure 6: Rear panel of the Barracuda SD-SDI encoder (B-280E-SDI)

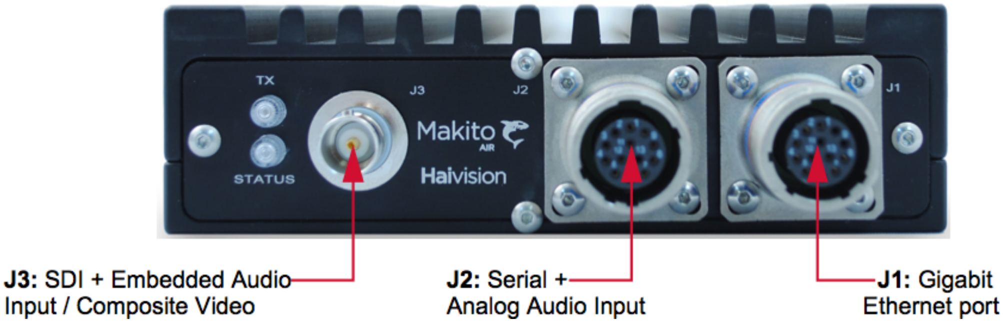

TX
STATUS
J3
J2
J1
Makito AIR
Haivision
J3: SDI + Embedded Audio Input / Composite Video
J2: Serial + Analog Audio Input
J1: Gigabit Ethernet port

Figure 7: Rear panel of the Makito Air ruggedized HD/SD encoder (S-290E-AIR and S-290E-AIR-COT)

Copyright © 2012 Haivision Network Video. All rights reserved. The Haivision logo, Furnace, Mako, Makito, Barracuda, Piranha, Stingray, InStream, Torpedo, Kraken, CoolSign, KulaByte and Hydra are trademarks of Haivision Network Video. Other trademarks in this document are the property of their respective owners. All specifications are subject to change without notice.

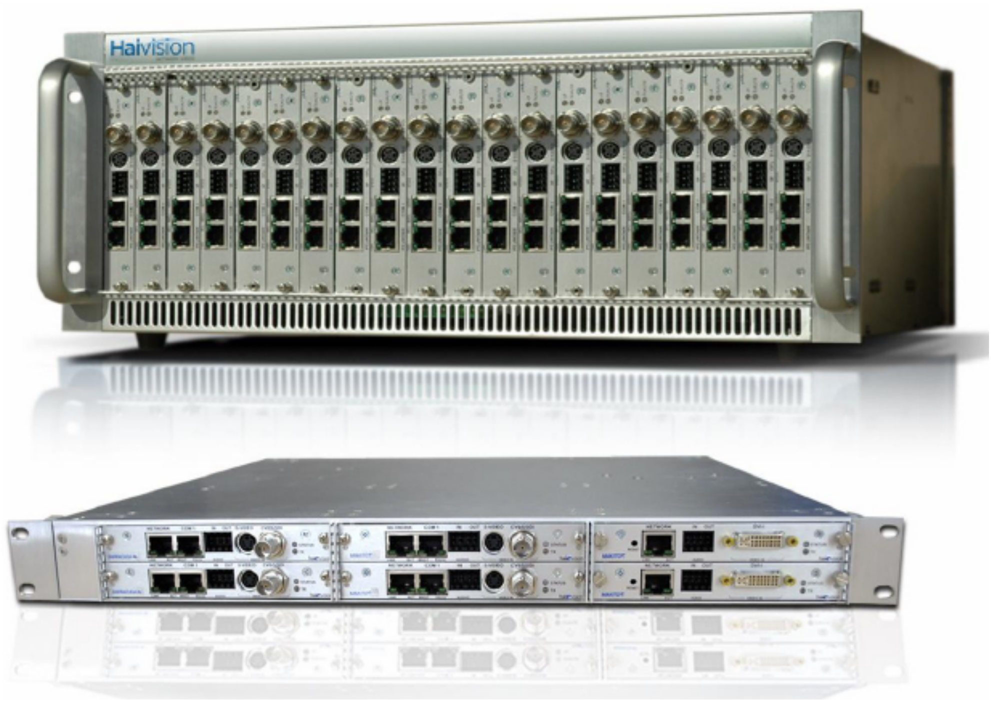


Figure 8: 21-slot and 6-slot chassis

> ***NOTE****: The Barracuda is an SD-only version of the Makito. Usage of the term Makito in this document shall be interpreted to include the Makito HD-SDI, the Makito DVI, the Makito AIR and the Barracuda. Use of the terms Makito HD-SDI, Makito DVI, Makito AIR or Barracuda either singularly or in multiples, shall be interpreted to include only the products specifically named.*

2.2.1 Usage and major security features of the TOE

The TOE encodes audio, video, and metadata into media streams that are transmitted over a network using RTP, RTMP, TS-MPEG, or QuickTime. The TOE provides no security for the media streams (no privacy, no authenticity, and no integrity).

The TOE audit feature allows basic audits to be performed for security-related events, and securely transfers audit data to an external audit server.

The TOE protects itself from tampering via several mechanisms that are implemented by either the TOE or its operating environment. The TOE's operating system separates processes into independent domains, such that one process cannot access the memory space of another. The operating system cannot be modified, and interfaces are strictly controlled.

The TOE relies on physical security to protect data from unauthorized modification.

Copyright © 2012 Haivision Network Video. All rights reserved. The Haivision logo, Furnace, Mako, Makito, Barracuda, Piranha, Stingray, InStream, Torpedo, Kraken, CoolSign, KulaByte and Hydra are trademarks of Haivision Network Video. Other trademarks in this document are the property of their respective owners. All specifications are subject to change without notice.

The TOE can be securely administered remotely through HTTPS/TLS (Web GUI) or SSH (CLI). All administrative users must be identified and authenticated by the TOE. Inactive interactive sessions are terminated after a Security Administrator-specified time period. The TOE supports role-based authorization for management functions.

The TOE can maintain reliable time stamps for the audit records. However, since it contains no battery backup real time clock, the date and time shall be initialized at startup time, with an external NTP server.

2.2.1.1 TOE Documentation

Haivision Systems Inc. produces several documents that describe the installation, configuration and use of the TOE, as well as guidance on its security features. The final documentation will be available online at https://www.haivision.com/download-center (registration required).

2.2.2 TOE Type

The TOE is a device used to encode incoming audio and video signals in a digital form suitable for streaming via Internet protocols.

2.2.3 TOE IT Environment

The TOE relies on external IT entities in the operating environment for its secure management.

The TOE supports syslog and can utilize an external audit server to store audit records.

The TOE supports NTP and must use an external time server to initialize its date and time at startup in order to time stamp audit records, validate certificates, and manage password aging.

A remote administrative user can use a web browser to access the Web GUI interface, or use a telnet or an SSH client to access the CLI. A local administrative user can use a terminal client on the serial port to access the CLI. Neither the web browser or the SSH client is part of the TOE. Note that the TOE supports telnet, but it cannot be used to access the TOE in the CC evaluated configuration. The TOE also includes an SNMPv3 agent that is not part of this CC evaluation since the applicable Protection Profile has no such provision.

The TOE does not support external authentication servers to authenticate administrative users.

For more information on the TOE environment please see the user documentation.

Copyright © 2012 Haivision Network Video. All rights reserved. The Haivision logo, Furnace, Mako, Makito, Barracuda, Piranha, Stingray, InStream, Torpedo, Kraken, CoolSign, KulaByte and Hydra are trademarks of Haivision Network Video. Other trademarks in this document are the property of their respective owners. All specifications are subject to change without notice.

2.3 TOE Description

2.3.1 Physical Scope of the TOE

2.3.1.1 Product Overview

The TOE delivers high performance H.264 encoding based on a compact and cost-effective blade form factor. It offers the ability to deliver multiple streams at different resolutions and bitrates to multiple destinations. It also supports both balanced and unbalanced stereo audio inputs as well as digital audio embedded within an SDI signal.

The Makito HD-DVI supports HD up to 1080p60 (Component Analog or Digital) or computer resolutions up to 1280x1024 at 75 Hz (RGB or DVI-D) input via its DVI-I connector.

The Makito HD-SDI supports SDI, HD-SDI, 3G-SDI (the new standard for 1080p60), and Composite on its BNC interface. The Makito-SDI also supports S-Video (for Standard Definition). Thus the Makito addresses video-over-IP encoding anywhere on a resolution / bandwidth scale from CIF as low as 150 kbps to full HD at 15 Mbps.

The Barracuda SDI accepts Composite, S-Video, and Serial Digital Interface (SDI) standard definition video inputs. The Barracuda can produce H.264 streams at full resolution and full frame rate at up to 8 Mbps, and yet with built-in downscaling and partial frame rate support can emit streams as low as 150 kbps.

2.3.1.2 Chassis Styles

Makito and Barracuda encoders (blades) can be installed in three types of passive chassis:

- an ultra-compact appliance chassis for single channel encoding
- within a 4U high density chassis that can contain up to 21 encoders
- within a 1U chassis that can contain up to 6 encoders

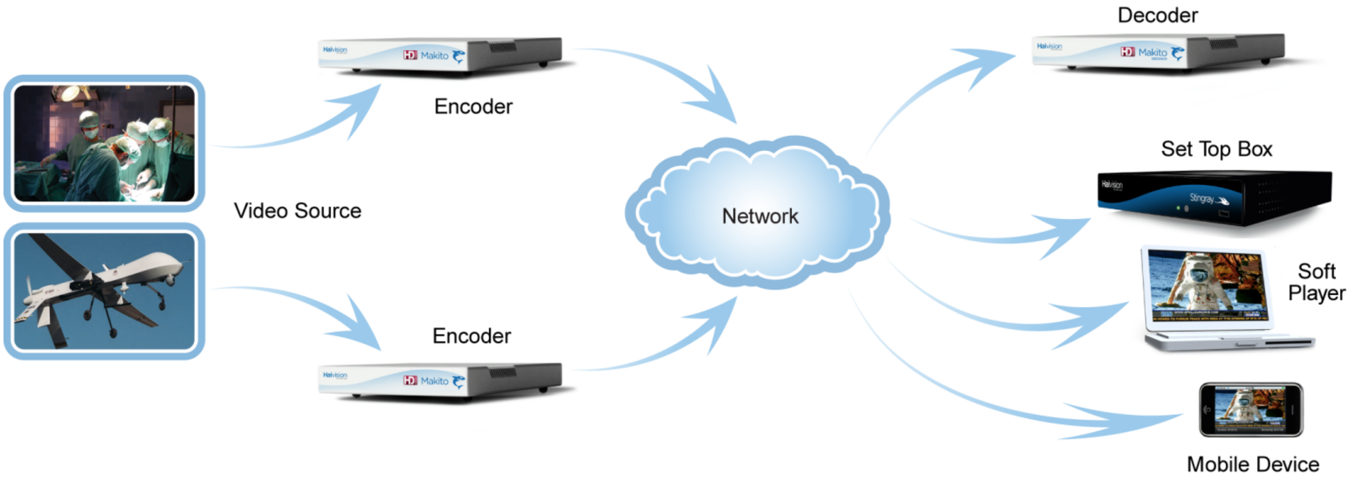
These chassis serve only to enclose the blades and provide power distribution.

2.3.1.3 Applications

Typical examples of Makito applications include:

- **IPTV Distribution** – delivering video channels to viewers in schools, financial institutions, live event venues, control rooms, and within government organizations.
- **Medical Systems** – driving video throughout healthcare facilities enabling education, consultation, and procedural review.
- **Streaming Services** – connecting facilities, affiliates, and event locations with real-time video, simultaneously addressing streaming and distribution challenges.

Copyright © 2012 Haivision Network Video. All rights reserved. The Haivision logo, Furnace, Mako, Makito, Barracuda, Piranha, Stingray, InStream, Torpedo, Kraken, CoolSign, KulaByte and Hydra are trademarks of Haivision Network Video. Other trademarks in this document are the property of their respective owners. All specifications are subject to change without notice.



2.3.1.4 Management Overview

All TOE interfaces and applications such as audio/video services and IP links may be configured, managed, and monitored remotely through its Ethernet LAN port using the Web interface, the Command Line Interface (CLI), or locally through the Serial Management port (if applicable) using the Command Line Interface (CLI).

Web Interface

Managing the TOE from the Web interface requires a connection from the unit's LAN port to a network. An administrative user can use a Web browser on a PC or other workstation to access the TOE's Web interface.

Command Line Interface (CLI)

Management via the CLI is possible from a remote location through SSH, or locally via an RS-232 console.

Copyright © 2012 Haivision Network Video. All rights reserved. The Haivision logo, Furnace, Mako, Makito, Barracuda, Piranha, Stingray, InStream, Torpedo, Kraken, CoolSign, KulaByte and Hydra are trademarks of Haivision Network Video. Other trademarks in this document are the property of their respective owners. All specifications are subject to change without notice.

2.3.2 Logical Scope of the TOE

The figure below depicts the logical scope of the TOE:

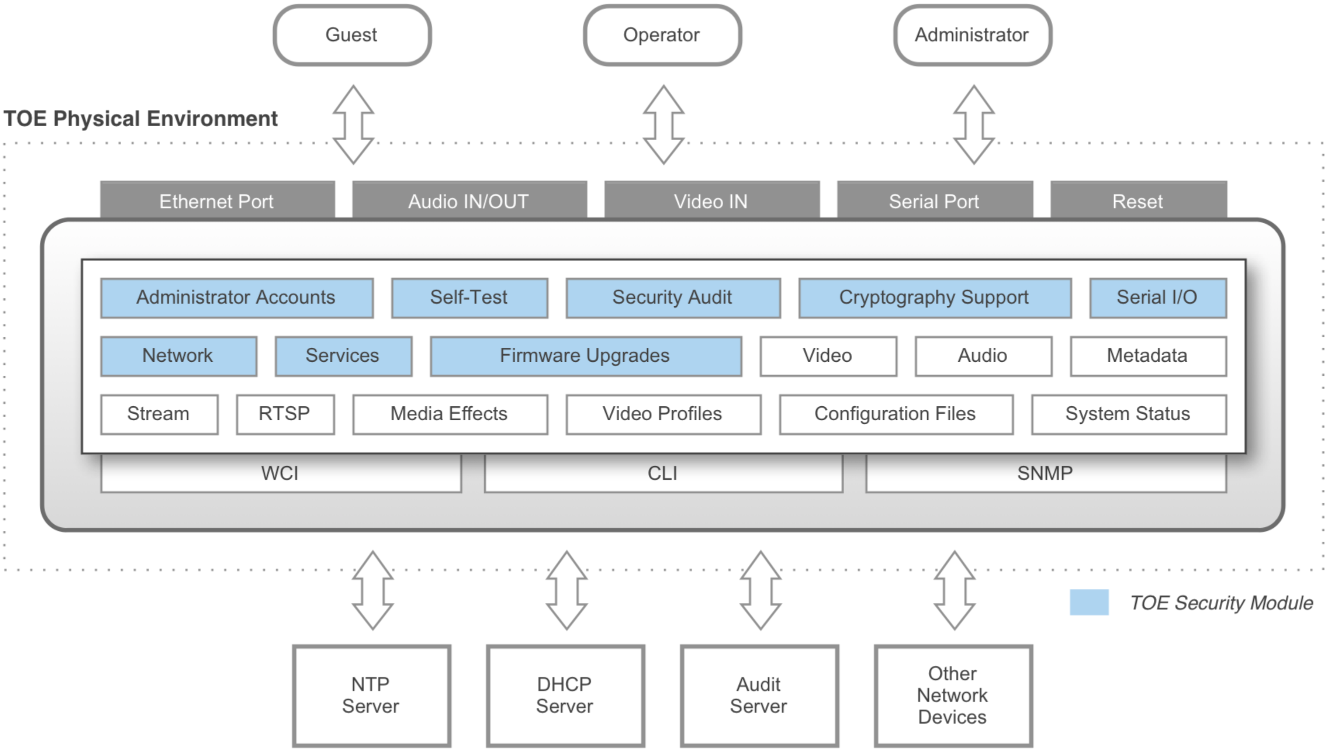


Figure 9: TOE Logical Scope

2.3.2.1 Role-based Authorization

The TOE provides functional module authorization to administrative users through three defined roles:

1. **Guest**: (guest administrator) provides read-only access to the system.
2. **Operator**: provides all rights to configure A/V and stream settings. However, it does not include rights to upgrade the system, modify the network settings, or manage accounts.
3. **Administrator**: provides all access rights and Security Administrator privileges and is hereafter called *Security Administrator*.

The table below describes role-based access to functional modules:

Copyright © 2012 Haivision Network Video. All rights reserved. The Haivision logo, Furnace, Mako, Makito, Barracuda, Piranha, Stingray, InStream, Torpedo, Kraken, CoolSign, KulaByte and Hydra are trademarks of Haivision Network Video. Other trademarks in this document are the property of their respective owners. All specifications are subject to change without notice.

Operation Module	Guest	Operator	Administrator
Video	X[1]	X	X
Audio	X[1]	X	X
Metadata	X[1]	X	X
Stream	X[1]	X	X
RTSP	X[1]	X	X
Media Effects	X[1]	X	X
Video Profiles	X[1]	X	X
Configuration Files	X[1]	X	X
System Status	X[1]	X	X
Security Module			
Network	X[1]	X[1]	X
Services			X
Administrative User Accounts			X
Cryptographic Support			X
Serial I/O			X
Self-Test			X
Security Audit			X
Firmware Upgrades			X

[1] *Read-only access*

Table 4: Role-based authorization to TOE functional modules settings

2.3.2.2 Physical I/O

The encoder appliance has five types of physical I/O interfaces:

1. **Ethernet Port**: used for IP-based communications over a LAN or WAN
2. **Audio IN/OUT**: used primarily for input of analog audio signals; audio output is supported only for the TalkBack function, which is disabled in the CC evaluated configurations.
3. **Video IN**: used for input of analog and/or digital video signals

Copyright © 2012 Haivision Network Video. All rights reserved. The Haivision logo, Furnace, Mako, Makito, Barracuda, Piranha, Stingray, InStream, Torpedo, Kraken, CoolSign, KulaByte and Hydra are trademarks of Haivision Network Video. Other trademarks in this document are the property of their respective owners. All specifications are subject to change without notice.

4. **Serial Port**: used as a management interface or for metadata input
5. **Reset Button**: used to trigger a firmware reset to factory default settings

2.3.2.3 Functional Modules

The encoder appliance has 17 functional modules. Only certain modules are considered to be part of the TSF. All modules are described here in order to provide context for the TOE functionality.

The following functional modules are part of the TSF:

1. **Administrative User Accounts**: used to manage administrative user accounts and assigned roles. The TOE has default administrative user accounts with login credentials, which must be changed at the time of installation.
2. **Self-Test**: used at boot-up time to self-test the security function to ensure no tampering has occurred.
3. **Security Audit**: used to manage the recognition, recording, and transmission-of information related to security activities.
4. **Cryptography Setting**: used to manage the cryptographic module and keys.
5. **Serial I/O**: used to manage the serial interface for either (1) connection to a computer for CLI control of the TOE, or (2) connection of the TOE to a metadata source.
6. **Network Settings**: used to manage the network interface settings for the TOE, including IP Address, DNS, and NTP.
7. **Services**: used to enable, disable, configure, and set the policies of the management interfaces (HTTP, SNMP, SSH, Telnet), as well as to enable or disable the following services: RTSP, Talkback, and VF. The Talkback, Telnet, and VF services are disabled for the CC evaluated configurations.
8. **Firmware Upgrades**: used to manage upgrades of the TOE firmware.

The following functional modules are ***not*** part of the TSF:

1. **Video**: used to manage the encoding settings properties such as the type, resolution, GOP size, and bit rate for video input.
2. **Audio**: used to manage the encoder's audio settings such as the number and type of audio channels and bit rate, as well for audio input via the TalkBack function.
3. **Metadata**: used to manage the capture of KLV (Key Length Value) metadata, and its incorporation within a transport stream. The TOE supports metadata input from the serial port (COM1), the HD-SDI interface, or an operator-definable UDP port. Only one metadata stream may be included in the transport stream at a time. This optional module is present when the SW-290E-KLV firmware option is installed.
4. **Stream**: used to manage the settings for the unicast or multicast output of up to 8 audio/video streams over IP, as well as their control (start, stop, pause, resume,

Copyright © 2012 Haivision Network Video. All rights reserved. The Haivision logo, Furnace, Mako, Makito, Barracuda, Piranha, Stingray, InStream, Torpedo, Kraken, CoolSign, KulaByte and Hydra are trademarks of Haivision Network Video. Other trademarks in this document are the property of their respective owners. All specifications are subject to change without notice.

etc.); also provides the ability to enable or disable Session Announcement Protocol (SAP) messages.

5. **RTSP**: used to configure the TOE to interoperate with RTSP-based software players such as haiPLAY, QuickTime, VideoLan VLC, or Wowza Server (Flash) for real-time streaming.
6. **Media Effects**: used to configure media effects such as a logo overlay in the encoded video, the insertion of a static image when the stream is paused, and the ability to take snapshots of the video input.
7. **Video Profiles**: used to manage default and custom presets for video quality parameters, such as motion, image complexity, uniformity, and rate control buffer size, as they apply to a given context (e.g. sports video).
8. **Configuration Files**: used to manage operator-created configurations for non-TSF (audio, video, streams) settings, which can be saved in a text file in flash memory. A saved configuration can be loaded at startup.
9. **System Status**: provides status information about the hardware and software components, such as card status, card type, part number, serial number, system uptime, encoding chipset load (%), firmware version, firmware date, hardware version, and boot revision for the encoder. This module can also be used to reboot the encoder and to take a system snapshot.

2.3.3 TOE Security Function (TSF) Overview

The table below summarizes the security functions provided by the TOE.

Security Function	TOE Scope Description
Security Audit (FAU)	The TOE generates audit logs that consist of various auditable events or actions. This includes logins, use of trusted channel/path, and cryptographic operations. Each audit event contains an associated date and time stamp, a label for the type of event, a user ID (if applicable), and a description of the event. The TOE relies on a syslog server to store and protect the audit history. The TOE outputs logs to an external audit server, but does not record audit events internally, and does not offer the ability to read external logs.
Cryptographic Support (FCS)	The cryptographic module protects the management interfaces (SSH, HTTPS). It employs RNG, key generation and establishment, zeroization, encryption, digital signature, and hashing algorithms.
User Data Protection (FDP)	The TOE ensures that audio/video media content (user data) does not leak outside of the streaming process.

Copyright © 2012 Haivision Network Video. All rights reserved. The Haivision logo, Furnace, Mako, Makito, Barracuda, Piranha, Stingray, InStream, Torpedo, Kraken, CoolSign, KulaByte and Hydra are trademarks of Haivision Network Video. Other trademarks in this document are the property of their respective owners. All specifications are subject to change without notice.

Security Function	TOE Scope Description
Identification and Authentication (FIA)	The TOE requires administrative users to be identified and authenticated (via username and password, or public key) prior to performing any operations. The TOE's administrative user accounts module maintains administrative user credentials and assigns roles to authenticated administrative users. Passwords of 15 characters or more are supported.
Security Management (FMT)	The TOE gives the Security Administrator (with appropriate access privileges) the ability to manage the security functions: auditing operations, administrative user accounts, password and session policies, advisory banners, software updates, as well as cryptographic functions. The TOE ensures that only secure values are accepted for security attributes. The Guest role has limited, read-only access to the management interfaces. The Operator role can manage audio, video, and streams but cannot manage security functions. The Administrator role (acting as the Security Administrator described in this document) can add, edit, change passwords and/or delete administrative user accounts. Other roles can change their own password, and view a limited number of security function settings.
Protection of the TSF (FPT)	The TOE prevents the unauthorized modification of TSF data. This protection includes self-tests to ensure the correct operation of cryptographic functions. A Security Administrator can also verify the integrity and authenticity of a firmware upgrade before installing it. The TOE relies on trusted channels to protect communications between itself and other trusted services, such as syslog. Communications between the TOE and a remote administrative user are protected via a trusted path.
TOE Access (FTA)	TOE *Security Administrators* can configure a maximum allowable period of inactivity for a user session. If there is no user interaction with the TOE for the specified amount of time, the session is terminated. The default session timeout, when enabled, is 15 minutes. The TOE also provides for a login banner message to be displayed by the management interfaces (Web GUI and CLI), to advise administrative users regarding the appropriate use of the TOE, and the penalty for its misuse.

Table 5: TOE Security Function (TSF) Overview

2.4 Conformance Claims (ASE_CCL)

2.4.1 Common Criteria Claims

The following conformance claims are made for the TOE and ST:

- **CC v3.1, Rev.3 conformant**
  The ST and TOE are conformant to Common Criteria version 3.1, revision 3.

Copyright © 2012 Haivision Network Video. All rights reserved. The Haivision logo, Furnace, Mako, Makito, Barracuda, Piranha, Stingray, InStream, Torpedo, Kraken, CoolSign, KulaByte and Hydra are trademarks of Haivision Network Video. Other trademarks in this document are the property of their respective owners. All specifications are subject to change without notice.

- **Part 2 extended**
  The ST is Common Criteria Part 2 extended.
- **Part 3 conformant**
  The ST is Common Criteria Part 3 conformant.
- **PP conformant**
  The ST complies to the NDPP (Protection Profile "Security Requirements for Network Devices"), Version 1.1, with additional requirements drawn from Appendix C of the NDPP.

Copyright © 2012 Haivision Network Video. All rights reserved. The Haivision logo, Furnace, Mako, Makito, Barracuda, Piranha, Stingray, InStream, Torpedo, Kraken, CoolSign, KulaByte and Hydra are trademarks of Haivision Network Video. Other trademarks in this document are the property of their respective owners. All specifications are subject to change without notice.

3. Security Problem Definition

This section describes the security aspects of the environment in which the TOE is to be used, as well as the expectations for its operation. This description is divided into three categories:

- **Assumptions** made about the operational environment and the manner in which the TOE is to be used
- **Threats** the be countered by the TOE and its environment
- **Organizational Security Policies** that define the security rules, procedures, or guidelines to be enforced by the TOE and its environment

3.1 Assumptions

The following assumptions about the operational environment are made regarding its ability to provide security functionality. If the TOE is placed in an operational environment that does not meet these assumptions, the TOE may not be able to provide all of its security functionality.

Assumption Name	Assumption Definition
A.NO_GENERAL_PURPOSE	It is assumed that there are no general-purpose computing capabilities (e.g., compilers or user applications) available on the TOE, other than those services necessary for the operation, administration and support of 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.TRUSTED_ADMIN	TOE administrative users are trusted to follow and apply all administrator guidance in a trusted manner.

Table 6: Assumptions

3.2 Threats

The table below describes the threats that are to be countered by the TOE, its operational environment, or a combination of the two.

Threat Name	Threat Definition
T.ADMIN_ERROR	An administrative user may unintentionally install or configure the TOE incorrectly, resulting in ineffective security mechanisms.

Copyright © 2012 Haivision Network Video. All rights reserved. The Haivision logo, Furnace, Mako, Makito, Barracuda, Piranha, Stingray, InStream, Torpedo, Kraken, CoolSign, KulaByte and Hydra are trademarks of Haivision Network Video. Other trademarks in this document are the property of their respective owners. All specifications are subject to change without notice.

Threat Name	Threat Definition
T.TSF_FAILURE	Security mechanisms of the TOE may fail, leading to a compromise of the TSF.
T.UNDETECTED_ACTIONS	Malicious remote users or external IT entities may take actions that adversely affect the security of the TOE. These actions may remain undetected and thus their effects cannot be effectively mitigated.
T.UNAUTHORIZED_ACCESS	A user may gain unauthorized access to the TOE data and TOE executable code. A malicious user, process, or external IT entity may masquerade as an authorized entity in order to gain unauthorized access to data or TOE resources. A malicious user, process, or external IT entity may misrepresent itself as the TOE to obtain identification and authentication data.
T.UNAUTHORIZED_UPDATE	A malicious party attempts to supply the end user with an update to the product that may compromise the security features of the TOE.
T.USER_DATA_REUSE	User data may be inadvertently sent to a destination not intended by the original sender.

Table 7: Threats

3.3 Organizational security policies (OSP)

The table below shows the OSPs that are to be enforced by the TOE, its operational environment, or a combination of the two.

Threat Name	Threat Definition
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 TOE.

Table 8: Organizational Security Policies

Copyright © 2012 Haivision Network Video. All rights reserved. The Haivision logo, Furnace, Mako, Makito, Barracuda, Piranha, Stingray, InStream, Torpedo, Kraken, CoolSign, KulaByte and Hydra are trademarks of Haivision Network Video. Other trademarks in this document are the property of their respective owners. All specifications are subject to change without notice.

4. Security Objectives (ASE_OBJ)

This section defines the security objectives for the TOE and its supporting environment. The security objectives are intended to counter identified threats, satisfy identified organizational security policies, and/or address assumptions.

4.1 Security Objectives for the TOE

Security objectives with respect to the TOE are summarized in the table below:

TOE Security Objective	TOE Security Objective Definition
O.PROTECTED_COMMUNICATIONS	The TOE will provide protected communication channels for administrative user and authorized IT entities.
O.VERIFIABLE_UPDATES	The TOE will provide the capability to help ensure that any updates to the TOE can be verified by the *Security Administrator* to be unaltered and (optionally) from a trusted source.
O.SYSTEM_MONITORING	The TOE will provide the capability to generate audit data and send those data to an external IT entity.
O.DISPLAY_BANNER	The TOE will display an advisory warning regarding use of the TOE.
O.TOE_ADMINISTRATION	The TOE will provide mechanisms to ensure that only administrative users are able to log in and configure the TOE, and provide protections for logged-in administrative users.
O.RESIDUAL_INFORMATION_CLEARING	The TOE will ensure that any data contained in a protected resource is not available when the resource is reallocated.
O.SESSION_LOCK	The TOE shall provide mechanisms that mitigate the risk of unattended sessions being hijacked.
O.TSF_SELF_TEST	The TOE will provide the capability to test some subset of its security functionality to ensure it is operating properly.

Table 9: TOE Security Objectives

4.2 Security Objectives for the Operational Environment (OE)

Certain objectives with respect to the general operating environment must be met for the TOE to meet its security functional requirements. Those objectives are described in the table below:

OE Security Objective	OE Security Objective Definition
OE.NO_GENERAL_PURPOSE	There are no general-purpose computing capabilities (e.g., compilers or user

Copyright © 2012 Haivision Network Video. All rights reserved. The Haivision logo, Furnace, Mako, Makito, Barracuda, Piranha, Stingray, InStream, Torpedo, Kraken, CoolSign, KulaByte and Hydra are trademarks of Haivision Network Video. Other trademarks in this document are the property of their respective owners. All specifications are subject to change without notice.

OE Security Objective	OE Security Objective Definition
	applications) available on the TOE, other than those services necessary for the operation, administration and support of the TOE.
OE.PHYSICAL	Physical security, commensurate with the value of the TOE and the data it contains, is provided by the environment.
OE.TRUSTED_ADMIN	TOE administrative users are trusted to follow and apply all administrative user guidance in a trusted manner.

Table 10: TOE Operational Environment Security Objectives

4.2.1 Operational Environment

The three operational environment security objectives OE.NO_GENERAL_PURPOSE, OE_PHYSICAL, and OE_TRUSTED_ADMIN, restate the corresponding assumptions (see section 2.1 Assumptions).

Copyright © 2012 Haivision Network Video. All rights reserved. The Haivision logo, Furnace, Mako, Makito, Barracuda, Piranha, Stingray, InStream, Torpedo, Kraken, CoolSign, KulaByte and Hydra are trademarks of Haivision Network Video. Other trademarks in this document are the property of their respective owners. All specifications are subject to change without notice.

4.3 Rationale for Security Objectives

This section demonstrates that each threat, organizational security policy, and assumption are mitigated by at least one security objective for the TOE, and that those security objectives counter the threats, enforce the policies, and uphold the assumptions.

Assumptions, Threats , and Policies	Security Objectives										
	O.PROTECTED_COMMUNICATIONS	O.VERIFIABLE_UPDATES	O.SYSTEM_MONITORING	O.DISPLAY_BANNER	O.TOE_ADMINISTRATION	O.RESIDUAL_INFORMATION_CLEARING	O.SESSION_LOCK	O.TSF_SELF_TEST	OE.NO_GENERAL_PURPOSE	OE.PHYSICAL	OE.TRUSTED_ADMIN
A.NO_GENERAL_PURPOSE									X		
A.PHYSICAL										X	
A.TRUSTED_ADMIN											X
T.ADMIN_ERROR			X		X				X		
T.TSF_FAILURE			X					X			
T.UNDETECTED_ACTIONS			X								
T.UNAUTHORIZED_ACCESS	X		X		X		X				
T.UNAUTHORIZED_UPDATE		X									
T.USER_DATA_REUSE						X					
P.ACCESS_BANNER				X							

Table 11: Completeness of Security Objectives

Copyright © 2012 Haivision Network Video. All rights reserved. The Haivision logo, Furnace, Mako, Makito, Barracuda, Piranha, Stingray, InStream, Torpedo, Kraken, CoolSign, KulaByte and Hydra are trademarks of Haivision Network Video. Other trademarks in this document are the property of their respective owners. All specifications are subject to change without notice.

4.3.1 Protected Communications

To address the issues concerning transmitting sensitive data to and from the TOE (T.UNAUTHORIZED_ACCESS), the TOE provides encryption for these communication paths between itself and the endpoint. These channels are implemented using SSH, TLS, and HTTPS. These protocols are specified by RFCs that offer a variety of implementation choices. Requirements have been imposed on some of these choices (particularly those for cryptographic primitives) to provide interoperability and resistance to cryptographic attack.

In addition to providing protection from disclosure (and detection of modification) for the communications, each of the protocols described in this document (SSH, TLS, and HTTPS) offers two-way authentication of each endpoint in a cryptographically secure manner, meaning that even if there was a malicious attacker between the two endpoints, any attempt to represent themselves to either endpoint of the communications path as the other communicating party would be detected. The requirements on each protocol, in addition to the structure of the protocols themselves, provide protection against replay attacks by including a unique value in each communication so that replay of that communication can be detected.

Related SFRs: FCS_CKM.1, FCS_CKM_EXT.4, FCS_COP.1(1), FCS_COP.1(2), FCS_COP.1(3), FCS_COP.1(4), FCS_RBG_EXT.1, FPT_SKP_EXT.1, FTP_ITC.1, FTP_TRP.1, (FCS_SSH_EXT.1, FCS_TLS_EXT.1, FCS_HTTPS_EXT.1)

4.3.2 Verifiable Updates

Failure by the *Security Administrator* to verify that updates to the system can be trusted may lead to compromise of the entire system (T.UNAUTHORIZED_UPDATE). To establish trust in the source of the updates, the TOE provides cryptographic mechanisms and procedures to procure the update, check the update cryptographically through the TOE-provided digital signature mechanism, and install the update on the system.

Related SFRs: FPT_TUD_EXT.1, FCS_COP.1(2), FCS_COP.1(3)

4.3.3 System Monitoring

In order to assure that information exists that allows *Security Administrators* to discover intentional and unintentional issues with the configuration and/or operation of the system (T.ADMIN_ERROR, T.UNDETECTED_ACTIONS), the TOE has the capability of generating audit data targeted at detecting such activity. Auditing of administrative activities provides information that may hasten corrective action should the system be configured incorrectly. Audit of select system events can provide an indication of failure of critical portions of the TOE (e.g., a cryptographic provider process not running (T.TSF_FAILURE)) or anomalous activity (e.g., establishment of an administrative session at a suspicious time, repeated failures to establish sessions or authenticate to the system) of a suspicious nature (T.UNAUTHORIZED_ACCESS).

In some instances there may be a large amount of audit information produced that could overwhelm the TOE or administrators in charge of reviewing the audit

Copyright © 2012 Haivision Network Video. All rights reserved. The Haivision logo, Furnace, Mako, Makito, Barracuda, Piranha, Stingray, InStream, Torpedo, Kraken, CoolSign, KulaByte and Hydra are trademarks of Haivision Network Video. Other trademarks in this document are the property of their respective owners. All specifications are subject to change without notice.

information. The TOE is capable of sending audit information to an external trusted entity, which mitigates the possibility that the generated audit data will cause some kind of denial of service situation on the TOE. This information carries reliable timestamps, which will help order the information when sent to the external device.

Loss of communication with the audit server is problematic. The TOE notifies the *Security Administrators* when this condition occurs.

Related SFRs: FAU_GEN.1, FAU_GEN.2, FAU_STG_EXT.1, FPT_STM.1

4.3.4 Banner

To apply the organization policies (P.ACCESS_BANNER), the TOE permits the *Security Administrators* to define and enable an access message that will be displayed before the login prompt or page.

Related SFRs: FTA_TAB.1

4.3.5 TOE Administration and Session Termination

In order to provide a trusted means for administrative users to interact with the TOE (T.UNAUTHORIZED_ACCESS), the TOE provides a password-based logon mechanism. The administrative user will have the capability to compose a strong password, and will have mechanisms in place so that the password must be changed regularly. To avoid attacks where an attacker might observe a password being typed by an administrative user, passwords are obscured during logon. Session termination is also be implemented to mitigate the risk of an account being used illegitimately. Passwords are stored in an obscured form, and there is no interface provided for specifically reading the password or password file such that the passwords are displayed in plain text.

Related SFRs: FIA_UIA_EXT.1, FIA_PMG_EXT.1, FIA_UAU.7, FMT_MTD.1, FMT_SMF.1, FMT_SMR.2, FPT_APW_EXT.1, FTA_SSL_EXT.1, FTA_SSL.3

4.3.6 Residual Information Clearing

In order to counter the threat that user data is inadvertently included in network traffic not intended by the original sender (T.USER_DATA_REUSE), the TSF ensures that network packets sent from the TOE do not include data "left over" from the processing of previous network information.

Related SFRs: FDP_RIP.2

4.3.7 TSF Self Test

In order to detect some number of failures of underlying security mechanisms used by the TSF (T.TSF_FAILURE), the TSF performs self-tests.

Related SFRs: FPT_TST_EXT.1

Copyright © 2012 Haivision Network Video. All rights reserved. The Haivision logo, Furnace, Mako, Makito, Barracuda, Piranha, Stingray, InStream, Torpedo, Kraken, CoolSign, KulaByte and Hydra are trademarks of Haivision Network Video. Other trademarks in this document are the property of their respective owners. All specifications are subject to change without notice.

5. Security Requirements

This section specifies the requirements for the TOE. The security functional requirements correspond to the security functions implemented by the TOE, as required by the PP.

5.1 TOE Security Functional Requirements (SFR)

This sub-section specifies the SFRs for the TOE. It organizes the SFRs by CC classes as per the table below.

CC Functional Class	TOE Security Functional Requirement	
FAU: Security Audit	FAU_GEN.1	Audit Data Generation
	FAU_GEN.2	User Identity Association
	FAU_STG_EXT.1	External Audit Trail Storage
FCS: Cryptographic Support	FCS_CKM.1	Cryptographic Key Generation (for asymmetric keys)
	FCS_CKM_EXT.4	Cryptographic Key Zeroization
	FCS_COP.1(1)	Cryptographic Operation (for data encryption/decryption)
	FCS_COP.1(2)	Cryptographic Operation (for cryptographic signature)
	FCS_COP.1(3)	Cryptographic Operation (for cryptographic hashing)
	FCS_COP.1(4)	Cryptographic Operation (for keyed-hash message authentication)
	FCS_RBG_EXT.1	Extended: Cryptographic Operation (Random Bit Generation)
	FCS_TLS_EXT.1	Explicit: TLS
	FCS_SSH_EXT.1	Explicit: SSH
	FCS_HTTPS_EXT.1	Explicit: HTTPS
FDP: User Data Protection	FDP_RIP.2	Full Residual Information Protection
FIA: Identification and Authentication	FIA_PMG_EXT.1	Password Management

Copyright © 2012 Haivision Network Video. All rights reserved. The Haivision logo, Furnace, Mako, Makito, Barracuda, Piranha, Stingray, InStream, Torpedo, Kraken, CoolSign, KulaByte and Hydra are trademarks of Haivision Network Video. Other trademarks in this document are the property of their respective owners. All specifications are subject to change without notice.

CC Functional Class	TOE Security Functional Requirement	
	FIA_UIA_EXT.1	User Identification and Authentication
	FIA_UAU_EXT.2	Extended: Password-based Authentication Mechanism
	FIA_UAU.7	Protected Authentication Feedback
FMT: Security Management	FMT_MTD.1	Management of TSF Data (for general TSF data)
	FMT_SMF.1	Specification of Management Functions
	FMT_SMR.2	Restrictions on Security Roles
FPT: Protection of the TSF	FPT_SKP_EXT.1	Extended: Protection of TSF Data (for reading of all symmetric keys)
	FPT_APW_EXT.1	Extended: Protection of Administrator Passwords
	FPT_STM.1	Reliable Time Stamps
	FPT_TUD_EXT.1	Extended: Trusted Update
	FPT_TST_EXT.1	TSF Testing
FTA: TOE Access	FTA_SSL_EXT.1	TSF-initiated Session Locking
	FTA_SSL.3	TSF-initiated Termination
	FTA_SSL.4	User-initiated Termination
	FTA_TAB.1	Default TOE Access Banners
FTP: Trusted Path/Channels	FTP_ITC.1	Inter-TSF Trusted Channel
	FTP_TRP.1	Trusted Path

Table 12: TOE Security Functional Requirements

5.1.1 Security Audit

5.1.1.1 FAU.GEN.1 — Audit Data Generation

FAU_GEN.1.1 The TSF shall be able to generate an audit record of the following auditable events:

- start-up and shutdown of the audit functions;
- all auditable events for the [*not specified*] level of audit;
- all administrative actions, and
- [*Specifically defined auditable events listed in the table below*]:

Copyright © 2012 Haivision Network Video. All rights reserved. The Haivision logo, Furnace, Mako, Makito, Barracuda, Piranha, Stingray, InStream, Torpedo, Kraken, CoolSign, KulaByte and Hydra are trademarks of Haivision Network Video. Other trademarks in this document are the property of their respective owners. All specifications are subject to change without notice.

SFR	Auditable Events	Additional Audit Record Contents
FAU_GEN.1	None.	
FAU_GEN.2	None.	
FAU_STG_EXT.1	None.	
FCS_CKM.1	None.	
FCS_CKM_EXT.4	None.	
FCS_COP.1(1)	None.	
FCS_COP.1(2)	None.	
FCS_COP.1(3)	None.	
FCS_COP.1(4)	None.	
FCS_RBG_EXT.1	None.	
FDP_RIP.2	None.	
FCS_PMG_EXT.1	None.	
FCS_TSL_EXT.1	Failure to establish a TLS Session. Establishment/Termination of a TLS session.	Reason for failure. Non-TOE endpoint of connection (IP address) for both successes and failures.
FCS_SSH_EXT.1	Failure to establish an SSH session Establishment/Termination of an SSH session	Reason for failure Non-TOE endpoint of connection (IP address) for both successes and failures.
FCS_HTTPS_EXT.1	Failure to establish a HTTPS Session. Establishment/Termination of a HTTPS session.	Reason for failure. Non-TOE endpoint of connection (IP address) for both successes and failures.
FIA_UIA_EXT.1	All use of the identification and authentication mechanism.	Provided user identity, origin of the attempt (e.g., IP address).
FIA_UAU_EXT.2	All use of the authentication mechanism.	Origin of the attempt (e.g., IP address).
FIA_UAU.7	None.	
FMT_MTD.1	None.	

Copyright © 2012 Haivision Network Video. All rights reserved. The Haivision logo, Furnace, Mako, Makito, Barracuda, Piranha, Stingray, InStream, Torpedo, Kraken, CoolSign, KulaByte and Hydra are trademarks of Haivision Network Video. Other trademarks in this document are the property of their respective owners. All specifications are subject to change without notice.

SFR	Auditable Events	Additional Audit Record Contents
FMT_SMF.1	None.	
FMT_SMR.2	None.	
FPT_SKP_EXT.1	None.	
FPT_APW_EXT.1	None.	
FPT_STM.1	Changes to the time.	The old and new values for the time. Origin of the attempt (e.g., IP address).
FPT_TUD_EXT.1	Initiation of update.	No additional information.
FPT_TST_EXT.1	None.	
FTA_SSL_EXT.1	Any attempts at unlocking of an interactive session.	No additional information.
FTA_SSL.3	The termination of a remote session by the session locking mechanism.	No additional information.
FTA_SSL.4	The termination of an interactive session.	No additional information.
FTA_TAB.1	None.	
FTP_ITC.1	Initiation of the trusted channel. Termination of the trusted channel. Failure of the trusted channel functions.	Identification of the initiator and target of failed trusted channels establishment attempt.
FTP_TRP.1	Initiation of the trusted channel. Termination of the trusted channel. Failures of the trusted path functions.	Identification of the claimed user identity.

Table 13: TOE Security Functional Requirements and Auditable Events

FAU_GEN.1.2 The TSF shall record within each audit record at least the following information:

- Date and time of the event, type of event, subject identity, outcome (success or failure) of the event; and
- For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [*information specified in column three of* Table 13].

Copyright © 2012 Haivision Network Video. All rights reserved. The Haivision logo, Furnace, Mako, Makito, Barracuda, Piranha, Stingray, InStream, Torpedo, Kraken, CoolSign, KulaByte and Hydra are trademarks of Haivision Network Video. Other trademarks in this document are the property of their respective owners. All specifications are subject to change without notice.

5.1.1.2 FAU_GEN.2 — User Identity Association

FAU_GEN.2.1 For audit events resulting from actions of identified users, the TSF shall be able to associate each auditable event with the identity of the user that caused the event.

5.1.1.3 FAU_STG_EXT.1 — External Audit Trail Storage

FAU_STG_EXT.1.1 The TSF shall be able to [*transmit the generated audit data to an external IT entity*] using a trusted channel implementing the [*TLS*] protocol.

5.1.2 Cryptographic Support (FCS)

5.1.2.1 FCS_CKM.1 — Cryptographic Key Generation (for asymmetric keys)

FCS_CKM.1.1 Refinement: The TSF shall generate asymmetric cryptographic keys used for key establishment in accordance with [[

- *NIST Special Publication 800-56B, “Recommendation for Pair-Wise Key Establishment Schemes Using Integer Factorization Cryptography” for RSA-based key establishment schemes*]

and specified cryptographic key sizes *equivalent to, or greater than, a symmetric key strength of 112 bits*.

5.1.2.2 FCS_CKM_EXT.4 — Cryptographic Key Zeroization

FCS_CKM_EXT.4.1 The TSF shall zeroize all plaintext secret and private cryptographic keys and CSPs when no longer required.

Application Note: “Cryptographic Critical Security Parameters” are defined in FIPS 140-2 as “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.”

The zeroization indicated above applies to each intermediate storage area for plaintext key/cryptographic critical security parameter (i.e., any storage, such as memory buffers, that is included in the path of such data) upon the transfer of the key/cryptographic critical security parameter to another location.

5.1.2.3 FCS_COP.1(1) — Cryptographic Operation (for data encryption/decryption)

FCS_COP.1.1(1): Refinement: The TSF shall perform [encryption and decryption] in accordance with a specified cryptographic algorithm [AES operating in [*CBC, CTR*]] and cryptographic key sizes 128-bits, 256-bits, and [*no other key sizes*] that meets the following:

- FIPS Pub 197, “Advanced Encryption Standard (AES)”
- [*NIST SP 800-38A*]

5.1.2.4 FCS_COP.1(2) — Cryptographic Operation (for cryptographic signature)

FCS_COP.1.1(2): Refinement: The TSF shall perform cryptographic signature services in accordance with a [*RSA Digital Signature Algorithm (rDSA) with a key size (modulus) of 2048 bits or greater*] that meets the following:

Copyright © 2012 Haivision Network Video. All rights reserved. The Haivision logo, Furnace, Mako, Makito, Barracuda, Piranha, Stingray, InStream, Torpedo, Kraken, CoolSign, KulaByte and Hydra are trademarks of Haivision Network Video. Other trademarks in this document are the property of their respective owners. All specifications are subject to change without notice.

- [*FIPS Pub 186-2 or FIPS Pub 186-3, “Digital Signature Standard”*]

5.1.2.5 FCS_COP.1(3) — Cryptographic Operation (for cryptographic hashing)

FCS_COP.1.1(3) Refinement: The TSF shall perform [cryptographic hashing services] in accordance with a specified cryptographic algorithm [*SHA-1, SHA-256*] and message digest sizes [160, *256*] bits that meet the following:

- FIPS Pub 180-3, “Secure Hash Standard”

5.1.2.6 FCS_COP.1(4) — Cryptographic Operation (for keyed-hash message authentication)

FCS_COP.1.1(4): Refinement: The TSF shall perform [keyed-hash message authentication] in accordance with a specified cryptographic algorithm:

- HMAC-[*SHA-1*] key size [160] and message digest sizes [160] bits,
- HMAC-[*SHA-256*] key size [256] and message digest size [256] bits,

that meet the following:

- FIPS Pub 198-1, "The Keyed-Hash Message Authentication Code, and FIPS Pub 180-3, “Secure Hash Standard.”

5.1.2.7 FCS_RBG_EXT.1 — Extended: Cryptographic Operation (Random Bit Generation)

FCS_RBG_EXT.1.1: The TSF shall perform all random bit generation (RBG) services in accordance with [*NIST Special Publication 800-90* using [*CTR_DRBG (AES)*]] seeded by an entropy source that accumulated entropy from [*a TSF-hardware-based noise source*].

FCS_RBG_EXT.1.2: The deterministic RBG shall be seeded with a minimum of [*256 bits*] of entropy at least equal to the greatest bit length of the keys and authorization factors that it will generate.

5.1.3 User Data Protection (FDP)

5.1.3.1 FDP_RIP.2 — Full Residual Information Protection

FDP_RIP.2.1: The TSF shall ensure that any previous information content of a resource is made unavailable upon the [*allocation of the resource to*] all objects.

5.1.4 Identification and Authentication (FIA)

5.1.4.1 FIA_PMG_EXT.1 — Password Management

FIA_PMG_EXT.1.1: The TSF shall provide the following password management capabilities for administrative passwords:

- Passwords shall be able to be composed of any combination of upper and lower case letters, numbers, and the following special characters: “!”, “@”, “#”, “$”, “%”, “^”, “&”, “*”, “(“, “)”, [“~”, “`”, “_”, “-”, “+”, “=”, “{“, “}”, “[“, “]”, “:”, “;”, “"”, “'”, “<”, “>”, “,”, “.”, “?”, “/”, “ “(space)];

Copyright © 2012 Haivision Network Video. All rights reserved. The Haivision logo, Furnace, Mako, Makito, Barracuda, Piranha, Stingray, InStream, Torpedo, Kraken, CoolSign, KulaByte and Hydra are trademarks of Haivision Network Video. Other trademarks in this document are the property of their respective owners. All specifications are subject to change without notice.

- Minimum password length shall be settable by the Security Administrator, and support passwords of 15 characters or greater;

5.1.4.2 FIA_UIA_EXT.1 — User Identification and Authentication

FIA_UIA_EXT.1.1: The TSF shall allow the following actions prior to requiring the non-TOE entity to initiate the identification and authentication process:

- Display the warning banner in accordance with FTA_TAB.1;
- [Access to the help pages on the web interface
- ICMP echo]

FIA_UIA_EXT.1.2: The TSF shall require each administrative user to be successfully identified and authenticated before allowing any other TSF-mediated actions on behalf of that administrative user.

Application Note: This requirement applies to users (administrators and external IT entities) of services available from the TOE directly, and not services available by connecting through the TOE. Authentication can be password-based through the local console or through a protocol that supports passwords (such as SSH), or be certificate based (SSH, TLS).

5.1.4.3 FIA_UAU_EXT.2 — Extended: Password-based Authentication Mechanism

FIA_UAU_EXT.2.1: The TSF shall provide a local password-based authentication mechanism, [*none*] to perform administrative user authentication.

5.1.4.4 FIA_UAU.7 — Protected Authentication Feedback

FIA_UAU.7.1: The TSF shall provide only obscured feedback to the administrative user while the authentication is in progress at the local console.

Application Note: “Obscured feedback” implies the TSF does not produce a visible display of any authentication data entered by a user (such as the echoing of a password), although an obscured indication of progress may be provided (such as an asterisk for each character). It also implies that the TSF does not return any information during the authentication process to the user that may provide any indication of the authentication data.

5.1.5 Security Management (FMT)

5.1.5.1 FMT_MTD.1 — Management of TSF data (for general TSF data)

FMT_MTD.1.1: The TSF shall restrict the ability to manage the TSF data to the *Security Administrators*.

Application Note: The word “manage” includes but is not limited to create, initialize, view, change default, modify, delete, clear, and append. This requirement is intended to be the “default” requirement for management of TSF data; other iterations of FMT_MTD should place different restrictions or operations available on the specifically-identified TSF data. TSF data includes cryptographic information as well; managing these data would include the association of a cryptographic protocol with an interface, for instance.

Copyright © 2012 Haivision Network Video. All rights reserved. The Haivision logo, Furnace, Mako, Makito, Barracuda, Piranha, Stingray, InStream, Torpedo, Kraken, CoolSign, KulaByte and Hydra are trademarks of Haivision Network Video. Other trademarks in this document are the property of their respective owners. All specifications are subject to change without notice.

5.1.5.2 FMT_SMF.1 — Specification of Management Functions

FMT_SMF.1.1: The TSF shall be capable of performing the following management functions:

- Ability to administer the TOE locally and remotely;
- Ability to update the TOE, and to verify the updates using [*digital signature*] capability prior to installing those updates;
- [
  - *Ability to configure the list of TOE services available before an entity is identified and authenticated, as specified in FIA_UIA_EXT.1;*
  - *Ability to configure the cryptographic functionality;*

  ]

5.1.5.3 FMT_SMR.2 — Restrictions on Security Roles

FMT_SMR.2.1: The TSF shall maintain the roles:

- Authorized Administrator.

FMT_SMR.2.2: The TSF shall be able to associate users with roles.

FMT_SMR.2.3: The TSF shall ensure that the conditions

- Authorized Administrator role shall be able to administer the TOE locally;
- Authorized Administrator role shall be able to administer the TOE remotely;

are satisfied.

5.1.6 Protection of the TSF (FPT)

5.1.6.1 FPT_SKP_EXT.1 — Extended: Protection of TSF Data (for reading of all symmetric keys)

FPT_SKP_EXT.1.1: Refinement: The TSF shall prevent reading of all pre-shared keys, symmetric key, and private keys.

Application Note: The intent of the requirement is that an administrator is unable to read or view the identified keys (stored or ephemeral) through “normal” interfaces. While it is understood that the administrator could directly read memory to view these keys, do so is not a trivial task and may require substantial work on the part of an administrator. Since the administrator is considered a trusted agent, it is assumed they would not endeavour in such an activity.

5.1.6.2 FPT_APW_EXT.1 — Extended: Protection of Administrator Passwords

FPT_APW_EXT.1.1: The TSF shall store passwords in non-plaintext form.

FPT_APW_EXT.1.2: The TSF shall prevent reading of the plaintext passwords.

5.1.6.3 FPT_STM.1 — Reliable Time Stamps

FPT_STM.1.1: The TSF shall be able to provide reliable time stamps for its own use.

Copyright © 2012 Haivision Network Video. All rights reserved. The Haivision logo, Furnace, Mako, Makito, Barracuda, Piranha, Stingray, InStream, Torpedo, Kraken, CoolSign, KulaByte and Hydra are trademarks of Haivision Network Video. Other trademarks in this document are the property of their respective owners. All specifications are subject to change without notice.

5.1.6.4 FPT_TUD_EXT.1 — Extended: Trusted Update

FPT_TUD_EXT.1.1: The TSF shall provide Security Administrators the ability to query the current version of the TOE firmware/software.

FPT_TUD_EXT.1.2: The TSF shall provide Security Administrators the ability to initiate updates to TOE firmware/software.

FPT_TUD_EXT.1.3: The TSF shall provide a means to verify firmware/software updates to the TOE using a [*digital signature mechanism*] prior to installing those updates.

Application Note: The digital signature mechanism referenced in the third element is one specified in FCS_COP.1(2).

5.1.6.5 FPT_TST_EXT.1 — TSF Testing

FPT_TST_EXT.1.1: The TSF shall run a suite of self tests during initial start-up (on power on) to demonstrate the correct operation of the TSF.

5.1.7 TOE Access (FTA)

5.1.7.1 FTA_SSL_EXT.1 — TSF-initiated Session Locking

FTA_SSL_EXT.1.1: The TSF shall, for local interactive sessions, [*terminate the session*] after a Security Administrator-specified time period of inactivity.

5.1.7.2 FTA_SSL.3 — TSF-initiated Termination

FTA_SSL.3.1: Refinement: The TSF shall terminate a remote interactive session after a [Security Administrator-configurable time interval of session inactivity]

5.1.7.3 FTA_SSL.4 — User-initiated Termination

FTA_SSL.4.1: The TSF shall allow Administrator-initiated termination of the Administrator’s own interactive session.

5.1.7.4 FTA_TAB.1 — Default TOE Access Banners

FTA_TAB.1.1: Refinement: Before establishing a user/administrator session the TSF shall display a Security Administrator-specified advisory notice and consent warning message regarding unauthorized use of the TOE.

Application Note: This requirement is intended to apply to interactive sessions between a human user and a TOE. IT entities establishing connections or programmatic connections (e.g., remote procedure calls over a network) are not covered by this requirement.

5.1.8 Trusted Path/Channels (FTP)

5.1.8.1 FTP_ITC.1 — Inter-TSF Trusted Channel

FTP_ITC.1.1: Refinement: The TSF shall use [*TLS*] to provide a trusted communication channel between itself and authorized IT entities supporting the following capabilities: audit server [*and no other*] that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from disclosure and detection of modification of the channel data..

Copyright © 2012 Haivision Network Video. All rights reserved. The Haivision logo, Furnace, Mako, Makito, Barracuda, Piranha, Stingray, InStream, Torpedo, Kraken, CoolSign, KulaByte and Hydra are trademarks of Haivision Network Video. Other trademarks in this document are the property of their respective owners. All specifications are subject to change without notice.

FTP_ITC.1.2: Refinement: The TSF shall permit the TSF, or the authorized IT entities to initiate communication via the trusted channel.

FTP_ITC.1.3: The TSF shall initiate communication via the trusted channel for [audit server].

5.1.8.2 FTP_TRP.1 — Trusted Path

FTP_TRP.1.1: Refinement: The TSF shall use [*SSH and HTTPS*] to provide a trusted communication path between itself and remote administrators that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from disclosure and detection of modification of the communication data.

FTP_TRP.1.2: Refinement: The TSF shall permit remote administrators to initiate communication via the trusted path.

FTP_TRP.1.3: Refinement: The TSF shall require the use of the trusted path for initial administrator authentication and all remote administration actions.

5.2 Additional Requirements

5.2.1 Additional Cryptographic Support (FCS)

5.2.1.1 FCS_TLS_EXT.1 — Explicit: TLS

FCS_TLS_EXT.1.1: The TSF shall implement one or more of the following protocols [*TLS 1.0 (RFC 2246), TLS 1.1 (RFC 4346), TLS 1.2 (RFC 5246)*] supporting the following ciphersuites:

Mandatory Ciphersuites:

- TLS_RSA_WITH_AES_128_CBC_SHA
- TLS_RSA_WITH_AES_256_CBC_SHA
- TLS_DHE_RSA_WITH_AES_128_CBC_SHA
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA

Optional Ciphersuites:

[

- *TLS_RSA_WITH_AES_128_CBC_SHA256*
- *TLS_RSA_WITH_AES_256_CBC_SHA256*
- *TLS_DHE_RSA_WITH_AES_128_CBC_SHA256*
- *TLS_DHE_RSA_WITH_AES_256_CBC_SHA256*

].

Copyright © 2012 Haivision Network Video. All rights reserved. The Haivision logo, Furnace, Mako, Makito, Barracuda, Piranha, Stingray, InStream, Torpedo, Kraken, CoolSign, KulaByte and Hydra are trademarks of Haivision Network Video. Other trademarks in this document are the property of their respective owners. All specifications are subject to change without notice.

5.2.1.2 FCS_SSH_EXT.1 — Explicit: SSH

FCS_SSH_EXT.1.1: The TSF shall implement the SSH protocol that complies with RFCs 4251, 4252, 4253, and 4254.

FCS_SSH_EXT.1.2: The TSF shall ensure that the SSH protocol implementation supports the following authentication methods as described in RFC 4252: public key-based, password-based.

FCS_SSH_EXT.1.3: The TSF shall ensure that, as described in RFC 4253, packets greater than [256 K] bytes in an SSH transport connection are dropped.

FCS_SSH_EXT.1.4: The TSF shall ensure that the SSH transport implementation uses the following encryption algorithms: AES-CBC-128, AES-CBC-256, and [*no other algorithms*].

FCS_SSH_EXT.1.5: The TSF shall ensure that the SSH transport implementation uses SSH_RSA and [*no other public key algorithms*] as its public key algorithm(s).

FCS_SSH_EXT.1.6: The TSF shall ensure that data integrity algorithms used in SSH transport connection are [*hmac-sha1*].

FCS_SSH_EXT.1.7: The TSF shall ensure that diffie-hellman-group14-sha1 is the only allowed key exchange method used for the SSH protocol.

5.2.1.3 FCS_HTTPS_EXT.1 — Explicit: HTTPS

FCS_HTTPS_EXT.1.1: The TSF shall implement the HTTPS protocol that complies with RFC 2818.

FCS_HTTPS_EXT.1.2: The TSF shall implement HTTPS using TLS as specified in FCS_TLS_EXT.1.

5.3 TOE Security Assurance Requirements

The TOE meets the security assurance requirements of NDPP v1.1. The following table is the summary of the requirements:

Assurance Class	Assurance Components	Assurance Components Description
ADV: Development	ADV_FSP.1	Basic Functional Specification
AGD: Guidance documents	AGD_OPE.1 AGD_PRE.1	Operational User Guidance Preparative User Guidance
ATE: Tests	ATE_IND.1	Independence Testing – Conformance
AVA: Vulnerability assessment	AVA_VAN.1	Vulnerability Analysis
ALC: Life Cycle Support	ALC_CMC.1 ALC_CMS.1	Labeling of the TOE TOE CM coverage

Table 14: TOE Security Assurance Requirements

Copyright © 2012 Haivision Network Video. All rights reserved. The Haivision logo, Furnace, Mako, Makito, Barracuda, Piranha, Stingray, InStream, Torpedo, Kraken, CoolSign, KulaByte and Hydra are trademarks of Haivision Network Video. Other trademarks in this document are the property of their respective owners. All specifications are subject to change without notice.

5.3.1.1 ALC_CMC.1 — Labeling of the TOE

The TOE labeling is provided by software. The Security Administrator can verify the hardware model, card type, hardware version, and firmware version using the CLI `haiversion` command or the WCI Status page.

Copyright © 2012 Haivision Network Video. All rights reserved. The Haivision logo, Furnace, Mako, Makito, Barracuda, Piranha, Stingray, InStream, Torpedo, Kraken, CoolSign, KulaByte and Hydra are trademarks of Haivision Network Video. Other trademarks in this document are the property of their respective owners. All specifications are subject to change without notice.

6. TOE Summary Specification (TSS)

The TOE Summary Specification (TSS) enables evaluators and potential consumers to gain a general understanding of how the TOE is implemented. The table below summarizes the TSFs matching the SFRs:

	TOE Security Functions							
	Security Audit	Cryptographic Support	User Data Protection	Identification and Authentication	Security Management	Protection of the TSF	TOE Access	Trusted Path/Channels
Security Functional Requirements								
FAU_GEN.1	X							
FAU_GEN.2	X							
FAU_STG_EXT.1	X	X						
FCS_CKM.1		X						
FCS_CKM_EXT.4		X						
FCS_COP.1(1)		X						
FCS_COP.1(2)		X						
FCS_COP.1(3)		X						
FCS_COP.1(4)		X						
FCS_RBG_EXT.1		X						
FCS_TLS_EXT.1		X						X
FCS_SSH_EXT.1		X						X
FCS_HTTPS_EXT.1		X						X
FDP_RIP.2			X					
FIA_PMG_EXT.1				X				
FIA_UIA_EXT.1				X				
FIA_UAU_EXT.2				X				
FIA_UAU.7				X				
FMT_MTD.1					X			
FMT_SMF.1					X			
FMT_SMR.2					X			
FPT_SKP_EXT.1						X		
FPT_APW_EXT.1						X		
FPT_STM.1						X		
FPT_TUD_EXT.1						X		
FPT_TST_EXT.1						X		

Copyright © 2012 Haivision Network Video. All rights reserved. The Haivision logo, Furnace, Mako, Makito, Barracuda, Piranha, Stingray, InStream, Torpedo, Kraken, CoolSign, KulaByte and Hydra are trademarks of Haivision Network Video. Other trademarks in this document are the property of their respective owners. All specifications are subject to change without notice.

	TOE Security Functions							
Security Functional Requirements	Security Audit	Cryptographic Support	User Data Protection	Identification and Authentication	Security Management	Protection of the TSF	TOE Access	Trusted Path/Channels
FTA_SSL_EXT.1							X	
FTA_SSL.3							X	
FTA_SSL.4							X	
FTA_TAB.1							X	
FTP_ITC.1								X
FTP_TRP.1								X

Table 15: TOE Summary Specification Overview

The sections below provide a more detailed description of the general technical mechanisms that the TOE uses to address the required Security Functions (see also section 1.3.2). Refer to the User's Guide and/or Hardening Guide for the CLI commands and WCI pages mentioned in these sections.

6.1 TOE Security Functions

6.1.1 Security Audit

The TOE has an audit function to record administrative and operational events.

The TOE generates audit records for auditable events. The audit records are transmitted to an external audit (syslog) server over a trusted channel (TLS), and are stored and protected by the audit server. The TOE does not provide an interface to read audit logs. The TOE does not store audit records locally.

The audit function is enabled and configured using the CLI `audit` command or the WCI Audit page. The audit function uses the TOE identity certificate for the TLS connection with the remote audit server. The TOE identity certificate and trusted root certificates are managed using the CLI `certificate` command or WCI Certificates page.

For each audit event, the information recorded includes:

- Event Type
- Subject Identity
- Date and Time
- Outcome

The following minimum events are audited:

- Administrative events:
    - Audit started

Copyright © 2012 Haivision Network Video. All rights reserved. The Haivision logo, Furnace, Mako, Makito, Barracuda, Piranha, Stingray, InStream, Torpedo, Kraken, CoolSign, KulaByte and Hydra are trademarks of Haivision Network Video. Other trademarks in this document are the property of their respective owners. All specifications are subject to change without notice.

  - Enabling/disabling services (ssh, telnet, vf, etc.)
  - System shutting down
  - System being rebooted
  - Installing a firmware upgrade
  - Changing network settings
  - Managing administrative user accounts, changing passwords
  - Administrative users logging in via CLI or WCI
  - Administrative users logging out (or being forced out after timeout)
- Operational events (both the request and the result are logged):
  - Configuration of video encoder parameters (GOP, bitrate, etc.)
  - Changing of video encoder admin status (start, stop, reset)
  - Configuration of audio encoder (algorithm, bitrate)
  - Changing of audio encoder admin status (start, stop)
  - Creation of streams
  - Deletion of streams
  - Changing of stream admin state (start, stop, pause, resume)
  - Creation of metadata sources
  - Deletion of metadata sources
  - Changing of metadata source admin state (start, stop)
  - Changing usage of serial port (console or metadata source)
  - Configuration of serial port parameters when used as metadata source (baudrate, protocol)
  - Conversion of pictures to logo format
  - Conversion of pictures to still image format
  - Configuration of logo feature
  - Application of video profile
  - Creation of video profile
  - Deletion of video profile
  - Loading of a saved configuration.
  - Saving a configuration

The Security Audit function is designed to satisfy the following security functional requirements:

- **FAU_GEN.1**: The TOE generates audit events. The events include startup of the audit function, all authentication attempts, all administrative actions, and all required auditable events as specified in Table 13. At a minimum, each event includes date and time, logging level (event type), subject identity, and outcome of event.
- **FAU_GEN.2:** The TOE associates user ID to the appropriate audit event. In other words, the user is identified by the username in the audit record.

Copyright © 2012 Haivision Network Video. All rights reserved. The Haivision logo, Furnace, Mako, Makito, Barracuda, Piranha, Stingray, InStream, Torpedo, Kraken, CoolSign, KulaByte and Hydra are trademarks of Haivision Network Video. Other trademarks in this document are the property of their respective owners. All specifications are subject to change without notice.

- **FAU_STG_EXT.1**: The TOE transmits the generated audit records to a remote syslog server using TCP over a TLS protected channel. The TOE notifies the *Security Administrators* on his/her next CLI login and on the web interface messages page, and stops transmitting audit records when the connectivity to the remote audit server is lost.

6.1.2 Cryptographic Support

The TOE uses the OpenSSL FIPS Object Module Version 2.0 to provide the cryptographic support for the CC evaluated configuration.

Table 16 below lists the supported algorithms, and the options used on the TOE.

Function	Algorithm	Options	CAVP Cert.
Random Number Generation	[SP 800-90] DRBG	CTR DRBG (AES)	#298
Encryption / Decryption	[FIPS Pub 197] AES	128/256 CBC, CTR	#2349
Message Digests	[FIPS Pub 180-3]	SHA-1, SHA-2 (256)	#2025
Keyed Hash	[FIPS Pub 198] HMAC	SHA-1, SHA-2 (256)	#1456
Digital Signature	[FIPS Pub 186-2] RSA	SigGen9.31, SigGenPKCS1.5, SigVer9.31, SigVerPKCS1.5	#1232
Asymmetric Key Generation	[FIPS Pub 186-3] RSA	186-3KeyGen: FIPS186-3_Fixed_e , FIPS186-3_Fixed_e_Value PGM(ProbRandom: (2048 , 3072) PPTT:(C.2)	#1211

Table 16: Cryptographic Support – OpenSSL FIPS Object Module Approved Algorithms

The TOE has not been FIPS 140-2 validated. The OpenSSL FIPS Object Module Version 2.0 has not been FIPS validated for the operational environment of the TOE (ARMv5TEJ w/ Linux 2.6) but the algorithms required by this Security Target have been validated for the TOE and the CAVP certificates obtained are listed in Table 16.

The OpenSSL FIPS Object Module is linked to the mainstream OpenSSL v1.0.1c shared library which provided not-validated FIPS-approved and non-approved cryptographic algorithms. When the TOE operates in FIPS mode for the CC evaluated configuration, only FIPS-approved algorithms are allowed for cryptographic services (e.g., encryption, hashing, digital signature, random number generation, etc.).

All use of the cryptographic module services (e.g., TLS 1.x, SSHv2, HTTPS, syslog, Firmware Upgrade digital signature, etc.) can only utilize FIPS-approved algorithms for the underlying algorithms.

The Cryptographic Support function is designed to satisfy the following security functional requirements. Unless otherwise specified, compliances claimed in this section (ex: FIPS Pub 197) are claims from the OpenSSL FIPS Object Module v2.0 Security Policy:

Copyright © 2012 Haivision Network Video. All rights reserved. The Haivision logo, Furnace, Mako, Makito, Barracuda, Piranha, Stingray, InStream, Torpedo, Kraken, CoolSign, KulaByte and Hydra are trademarks of Haivision Network Video. Other trademarks in this document are the property of their respective owners. All specifications are subject to change without notice.

- **FCS_CKM.1**: The TSF generates 2048-bit RSA keys, which are equivalent or greater in strength to 112 bit symmetric keys, using random numbers generated in accordance with NIST SP 800-90 (CTR_DRBG with AES-256).

  The TSF complements the OpenSSL cryptographic module for RSA key generation to support validation against FIPS Pub 186-3 (OpenSSL only supports FIPS Pub 186-2 RSA Key Generation). The options of the TSF RSA key generation of the NIST SP 800-56B sections pertinent to key generation (§5.3, §5.4, §5.5, §6.2, §6.3.1) are listed in Table 17, followed by the required sections of FIPS Pub 186-3 Appendix B.3 in Table 18.

SP 800-56B	Requirements	TSF Implementation & Differences
5. Cryptographic Elements		
5.3 Random Bit Generation		
§5.3	approved random bit generator (RBG)	See FCS_RBG_EXT.1
5.4 Prime Number Generator		
§5.4	approved prime factor generator	See table 18
5.5 Primality Testing Methods		
§5.5	approved primality testing method	See table 18
6. RSA Key Pairs		
6.2 Criteria for RSA Key Pairs for Key Establishment		
6.2.2 Formats		
§6.2.2	One of: basic, prime factor, or CRT format	CRT format
6.2.3 Parameter Length Sets		
§6.2.3	One of: 80 bits, 112 bits security strength	Only 2048 bit RSA Keys (112 bits security strength) are generated. MAC used for generated key verification is sha256.
6.3 RSA Key Pair Generators		
§6.3.1	RSAKPG1 Family: Fixed Public Exponent Three representations: 1) basic, 2) prime factor, or 3) CRT.	Fixed Public Exponent with CRT format
§6.3.1.3(1) - step 2	prime factor generation	See table 18
§6.3.1.3 - step 6	pair-wise consistency test: $k = (k^e)^d \bmod n$	Pair-wise consistency test (k=2) performed along with three signatures generation and verification (x9.31, pkcs1, pss), plus encryption/decryption.

Table 17: SP 800-56B RSA Key Generation – TSF Implementation and Differences

Copyright © 2012 Haivision Network Video. All rights reserved. The Haivision logo, Furnace, Mako, Makito, Barracuda, Piranha, Stingray, InStream, Torpedo, Kraken, CoolSign, KulaByte and Hydra are trademarks of Haivision Network Video. Other trademarks in this document are the property of their respective owners. All specifications are subject to change without notice.

FIPS 186-3	Requirements	TSF Implementation & Differences
B.3. IFC Key Pair Generation		
B.3.1 Criteria for IFC Key Pairs		
§B.3.1	A-1. Provable primes, or A-2. Probable primes, or B-1..B.3. Primes with Conditions	A-2. Probable primes
B.3.3 Generation of Random Primes that are Probably Prime		

§B.3.3 - Input	nBits
	e
		nBits = 2048
		e = 65537 (fixed)

B.3.3 - 4 Generate p:		
§B.3.3 – 4.3	If (p is not odd), then p = p + 1	If (p is not odd), then p = p + 1 While (p and p-1 are not relatively prime to the first 2048 prime numbers except 2), do p = p + 2.
§B.3.3 – 4.5.1	Primality test from Appendix C.3	See §C.3.1
B.3.3 - 5 Generate q:		
§B.3.3 – 5.3	If (q is not odd), then q = q + 1	If (q is not odd), then q = q + 1 While (q and q-1 are not relatively prime to the first 2048 prime numbers except 2), do q = q + 2.
§B.3.3 – 5.6.1	Primality test from Appendix C.3	See §C.3.1
C.3.1 Miller-Rabin Probabilistic Primality Test		
§C.3.1 – Input	Minimum number of rounds of M-R testing Table C.2: p and q 1024 bits: error = 2^{-112}: iterations = 5	iterations for p and q = 5

Table 18: FIPS 186-3 RSA Key Generation – TSF Implementation and Differences

The following CLI command can be used to run the RSA2VS KeyGen_RandomProbablyPrime3_3 test:

```
rsa2vs_ptest infile.req outfile.rsp
```

The RSA2VS Known Answer Test is not supported and not required since the TSF RSA key generator uses a fixed public exponent (e).

RSA keys are generated for the SSH management interface, self-signed X.509 certificate, and Certificate Signing Requests for TLS (Audit, HTTPS).

- **FCS_CKM_EXT.4**: All keys and secret data generated by the cryptographic module for the secure applications are automatically overwritten with random bytes before their memory is freed when they are no longer required or when they are released by the secure application.

Copyright © 2012 Haivision Network Video. All rights reserved. The Haivision logo, Furnace, Mako, Makito, Barracuda, Piranha, Stingray, InStream, Torpedo, Kraken, CoolSign, KulaByte and Hydra are trademarks of Haivision Network Video. Other trademarks in this document are the property of their respective owners. All specifications are subject to change without notice.

Private keys and password files maintained on the Flash-based file system (ext3 mounted with data=ordered) are deleted using the 'shred' Linux command: the file is stretched to the end of its last file system block, overwritten three times, overwritten another time with zeros, then truncated and deleted.

The following private keys are present on the CC evaluated configuration file system:

- SSH RSA private key (generated)
- TLS Certificates RSA private keys (generated with CSR or imported)

- **FCS_COP.1(1)**: The cryptographic module supports FIPS Pub 197 AES in the CBC and CTR modes with 128 and 256 bit keys.

  The following AVS CLI commands can be used to validate the AES algorithm:

  ```
  fips_algvs fips_aesavs -f infile.req outfile.rsp
  ```

  The AES-CBC encryption algorithm is used to encrypt data in TLS and SSH, and AES-CTR is used for deterministic random number generation (SP 800-90 CTR_DRBG).

- **FCS_COP.1(2)**: The TSF supports the FIPS Pub 186-2 RSA digital signature algorithm with a key size (modulus) of 2048 bits.

  RSA digital signature is used when installing firmware updates, validating certificates, on SSH Key Exchange, and for TLS (Audit, HTTPS).

  The following AVS CLI commands can be used to validate RSA signatures generation (rsastest) and verification (rsavtest) in the three supported schemes:

  X9.31:

  ```
  fips_algvs fips_rsastest -x931 infile.req outfile.req
  fips_algvs fips_rsavtest -x931 infile.req outfile.req
  ```

  RSASSA-PKCS1:

  ```
  fips_algvs fips_rsastest infile.req outfile.req
  fips_algvs fips_rsavtest infile.req outfile.req
  ```

  RSASSA-PSS:

  ```
  fips_algvs fips_rsastest -saltlen len ifile.req ofile.req
  fips_algvs fips_rsavtest -saltlen len ifile.req ofile.req
  ```

- **FCS_COP.1(3)**: The TSF supports FIPS 180-3 cryptographic hashing via the SHA1 or SHA-256 algorithm.

  The following AVS CLI command can be used to validate the SHA algorithm:

  ```
  fips_algvs fips_shatest infile.req outfile.rsp
  ```

Copyright © 2012 Haivision Network Video. All rights reserved. The Haivision logo, Furnace, Mako, Makito, Barracuda, Piranha, Stingray, InStream, Torpedo, Kraken, CoolSign, KulaByte and Hydra are trademarks of Haivision Network Video. Other trademarks in this document are the property of their respective owners. All specifications are subject to change without notice.

The cryptographic hash algorithm is used mainly for the support of keyed-hash message authentication (FCS_COP.1(4)), SSH key exchange (dh-group14-sha1) and digital signature (firmware upgrade).

- **FCS_COP.1(4)**: The TSF supports FIPS Pub 198-1 keyed-hash message authentication.

  The following AVS CLI command can be used to validate the HMAC algorithm:

  ```
  fips_algvs fips_hmactest infile.req outfile.rsp
  ```

  HMAC-SHA1 is used for SSH and TLS v1.x while HMAC-SHA-256 is also used for TLS v1.x ciphersuites.

- **FCS_RBG_EXT.1**: The TSF supports a SP 800-90 DRBG and is using the CTR_DRBG (AES) with a derivation function.

  The following AVS CLI command can be used to validate the DRBG algorithm:

  ```
  fips_algvs fips_drbgvs infile.req outfile.rsp
  ```

  Each secure application using the cryptographic module has its own instance of the DRBG. It is instantiated with 256 bits of strength by default, the highest security strength required by the TSF.

Applications	Protocols/Algorithms	Security Strength (SP 800-57)
HTTP/TLS	RSA 2048 AES-128/256, HMAC-SHA1/SHA-256	112 128/256 128/256
SSH	DH-group14-sha1 SSH_RSA AES-128/256 HMAC-SHA1	112 112 128/256 128
syslog/TLS	see HTTP/TLS	112, 128, 256
Firmware Signature	RSA 2048 SHA-256	112 128

Table 19: Cryptographic Support – Applications

The DRBG is seeded by a hardware-based noise source.

6.1.3 User Data Protection

There is no private user data per se transiting through the TOE. Users of the TOE are passive viewers/listeners of common media streams (MPEG-TS, RTP, RTMP, or QuickTime) encoded in real-time from the TOE audio, video, and metadata inputs, and transmitted unprotected on the network.

Copyright © 2012 Haivision Network Video. All rights reserved. The Haivision logo, Furnace, Mako, Makito, Barracuda, Piranha, Stingray, InStream, Torpedo, Kraken, CoolSign, KulaByte and Hydra are trademarks of Haivision Network Video. Other trademarks in this document are the property of their respective owners. All specifications are subject to change without notice.

The input signal is the same for all viewers/listeners and is considered to be the organization's data for which confidentiality, authenticity and integrity is not the responsibility of the TOE. Viewers/listeners of the media streams do not have to be identified users of the TOE. The knowledge of the multicast address (and the protocols) provides access to the content. If RTSP is enabled on the TOE, the knowledge of the URL of the media stream is enough to provide access to it.

This Security Target claims no protection of the media streams.

- **FDP_RIP.2**: In the context of the TOE, there is no transiting user data to protect but no data can leak between management sessions, or between management sessions and the audio/video streams.

  The Ethernet driver pads the output packet with zeros when its content is smaller than the minimum Ethernet packet (60 bytes) to prevent leaking data from other networking channels while using kernel network buffers.

  The audio/video stream is entirely processed within a single process (session manager). Since the system performs memory zeroization of new memory blocks allocated to a process at allocation time, no object outside session manager may contain the user data processed by session manager through dynamic memory obtained from the system. Dynamic memory is obtained from RAM and is zeroized by the system by writing a zero once in each of the allocated bytes.

  Each CLI-based SSH management session is handled by a separate SSH process. Each web interface HTTPS stateless request is processed in a separate process.

6.1.4 Identification and Authentication

The TSF maintains local administrative user name/password/role databases for interactive management sessions.

Security Administrators manage all administrative users' account with the CLI `account` command or the WCI Accounts page. Password policies are managed with the CLI `policy` (password) command or the WCI Policies page.

Password policies are not enforced by the TSF when *Security Administrators* create accounts or reset the password of other users' accounts. Instead, the password is forced to expire and the account owner is required to change its password upon next login.

Administrative users can change their own password using the CLI `passwd` command or the WCI My Account page (or their own Account page for *Security Administrators*), constrained by the password policies.

Administrative users can also manage their SSH authorized public keys using the CLI `pubkey` command or the WCI My Account page (or their own Account page for *Security Administrators*). *Security Administrators* can manage any administrative user's public keys with the CLI `account` command or the WCI Accounts page.

The Identification and Authentication function is designed to satisfy the following security functional requirements:

Copyright © 2012 Haivision Network Video. All rights reserved. The Haivision logo, Furnace, Mako, Makito, Barracuda, Piranha, Stingray, InStream, Torpedo, Kraken, CoolSign, KulaByte and Hydra are trademarks of Haivision Network Video. Other trademarks in this document are the property of their respective owners. All specifications are subject to change without notice.

- **FIA_PMG_EXT.1**: *Security Administrators* can define password policies for administrative user accounts: the password minimum length can be set up to 40 characters. Passwords of up to 80 characters are supported.

  While not required by the applicable Protection Profile, *Security Administrators* can also specify the required password composition (lowercase/uppercase letters, digits, symbols), and set a lifetime after which the administrative users are required to change their password.

- **FIA_UIA_EXT.1**: The TSF identifies and authenticates each administrative user before providing access to the CLI command prompt or WCI pages beyond the logon page (except the Advisory and Consent Banner and the help pages).

  Upon successful connection to the TOE, locally using the serial port (if enabled for management), or remotely using SSH (password-based authentication), users are prompted for their name and password. Only successful authentication will provide users a CLI command prompt, otherwise they will be prompted over and over again (with SSH disconnecting after 6 unsuccessful attempts).

  Upon successful connection to the TOE remotely using SSH with a public key that has been added to an administrative user account's authorized keys, user is granted access to the CLI command prompt without other formalities.

  Upon successful TLS connection to the WCI, the client web browser presents the user a login page, after consenting to the banner page if configured. The user must then enter its name and password. Only successful authentication will grant access to the TOE management pages beyond the login page.

- **FIA_UAU_EXT.2**: The TSF implements local password-based authentication and supports no remote (external) authentication mechanism.

  The TSF also support public key-based authentication when using SSH.

- **FIA_UAU.7**: The TSF obscures feedback when passwords are entered on the CLI login prompt or WCI logon page, and when they are modified with the CLI `account` and `passwd` commands or the WCI Accounts pages and the expired password pop-up dialog.

6.1.5 Security Management

TOE *Security Administrators* can create login accounts and assign them to one of the following roles: *Administrator*, *Operator*, or *Guest*. The CLI `account` command or the WCI Accounts page is used to create an administrative user account and assign it a role.

The TOE *Administrator* role maps to the *Security Administrator* role described in this document and the applicable Protection Profile.

The *Administrators* manage the TSF and the media streams. The *Operators* manage the media streams, and the *Guests* can only read the media stream configuration and monitor the status of the TOE.

All roles are permitted to log on the TOE using the CLI or the web interface (WCI), but their actions on the TOE are limited by their role (see Table 4).

Copyright © 2012 Haivision Network Video. All rights reserved. The Haivision logo, Furnace, Mako, Makito, Barracuda, Piranha, Stingray, InStream, Torpedo, Kraken, CoolSign, KulaByte and Hydra are trademarks of Haivision Network Video. Other trademarks in this document are the property of their respective owners. All specifications are subject to change without notice.

The Security Management function is designed to satisfy the following security functional requirements:

- **FMT_MTD.1**: Only *Administrators* are allowed to manage the TOE security functions. The other roles are optional and not required for the proper operation of the TOE. They are not involved in the TOE security functionality.
- **FMT_SMF.1**: The TOE permits the local and remote management of the TSF, including the cryptographic module and the validation and installation of the firmware upgrades.
- **FMT_SMR.2**: The *Administrator* role is the sole security role. Each administrative user is assigned one of the *Administrator*, *Operator*, or *Guest* role. *Administrators* can manage the TSF locally, via the serial port, or remotely using SSH or HTTPS.

6.1.6 Protection of the TSF

The TSF Data is mostly stored on a flash-memory based Linux file system, in files and databases that are readable and writable by the root user only.

The root account is not used to log in to the TOE and is locked down at the factory.

The ability to manage the TSF data is provided to the *Security Administrators* through the sudo Linux command for a limited set of operations.

The TOE flash-memory based file system is supported by a micro-SD device that can be ejected if the TOE enclosure is opened. The environment shall then provide physical security to the TOE as stipulated by the A.PHYSICAL assumption.

The firmware is based on the Linux operating system and proprietary applications that can be upgraded from digitally signed packages only.

The Protection of the TSF function is designed to satisfy the following security functional requirements:

- **FPT_SKP_EXT.1:** Private cryptographic keys (SSH, TLS) are stored in files that are neither readable nor writable by any administrative user.

  The TOE SSH host keys are generated by the TOE and only accessible to SSH and the root user.

  TLS certificates private keys generated by *Security Administrators* using the CLI `certificate` (create) command or WCI Certificates page are only accessible to the root user and TLS-based applications (Audit, HTTPS). They cannot be accessed or exported outside the TOE by any administrative user.

  TLS certificates can also be imported with their private key, password protected or not, using the CLI `certificate` (import) command or WCI Certificates page. Once on the Makito, these private keys are protected as for the generated keys but these keys are known outside the TOE and shall be protected by the environment.

Copyright © 2012 Haivision Network Video. All rights reserved. The Haivision logo, Furnace, Mako, Makito, Barracuda, Piranha, Stingray, InStream, Torpedo, Kraken, CoolSign, KulaByte and Hydra are trademarks of Haivision Network Video. Other trademarks in this document are the property of their respective owners. All specifications are subject to change without notice.

- **FPT_APW_EXT.1**: The TOE administrative user passwords are salted with an 8 characters random string and hashed using SHA-256 before being stored in the shadow database. The shadow database file is distinct from the password file (account database without passwords) that is readable by all for compatibility reasons. The shadow database is neither readable nor writable by any administrative user. *Security Administrators* can create and delete administrative user accounts and change their password but cannot perform any other operations on the password database.
- **FPT_STM.1**: The TOE implements reliable time stamps for audited events, passwords expiration, and X.509 certificates validation using the system date and time. The TOE has no battery backup hardware real time clock, therefore to preserve the monotonicity of audit records time stamp, the TOE uses NTP at startup to get the actual wall clock time to set the system date and time.

  The CLI `dtconfig` and `tzconfig` commands are used in the preparation procedures to set the date, time, and time zone. The CLI `ipconfig` command or the WCI Network page are use to setup the NTP server that is used at system startup to set the date, time, and time zone.

  The CLI `date` command is used to display the actual date, time, and timezone.
- **FPT_TUD_EXT.1**: The TSF implements firmware upgrade using digitally signed software packages.

  Registered customers with an upgraded account can download firmware upgrade packages from the Download Center of the Haivision web site (www.haivision.com).

  The package (ex: haios_enc_v2.1.1.hai) is a tar file containing components (ex: haios-oam_2.1.1-3.deb) that are individually signed (.sigv1). The TOE installed package version number and components can be listed with the CLI `package` (info) command. The CLI `package` command can also download (tftp), verify, and install the package. The WCI Upgrade page can upload the package and install it.

  Package components are hashed with SHA-256 and the digest is signed with a package signing certificate private key using X9.31 padding at firmware publication time. The package signing certificate is also included in the package.

  This package signing certificate is signed by the Haivision firmware root CA certificate that is pre-installed in each TOE to validate the package signing certificate. No administrative user can modify, delete, or replace this root CA certificate.

  The certificate and the components signature are validated when the package is downloaded (CLI) or uploaded (WCI) to the TOE. If validation succeeded, the package can be schedule for installation upon reboot using the CLI `package` (install) command or by continuing the installation on the WCI Upgrade page. The downloaded/uploaded package is deleted if the certificate is not valid or if any component signature is invalid.

Copyright © 2012 Haivision Network Video. All rights reserved. The Haivision logo, Furnace, Mako, Makito, Barracuda, Piranha, Stingray, InStream, Torpedo, Kraken, CoolSign, KulaByte and Hydra are trademarks of Haivision Network Video. Other trademarks in this document are the property of their respective owners. All specifications are subject to change without notice.

The certificate and signatures are validated again when the package is actually installed upon reboot. Installation is aborted if the certificate or any component signature is invalid and the installation error is logged (audited) and a message sent to *Security Administrators* (displayed upon CLI login and `messages` command, or on the WCI Messages page).

The pre-installed Haivision firmware root CA certificate verifies the package signing certificate. The package signing certificate verifies the package components digital signature. Both certificates are X.509, signed using sha256WithRSAEncryption, with an RSA public key of 2048 bits.

- **FPT_TST_EXT.1**: The heart of the TSF security is provided by the cryptographic module and its hardware-based noise source and they are the only components tested at startup. The cryptographic module self tests verify the integrity of the object module and the operation of the cryptographic algorithms. *Security Administrators* can run the cryptographic module power-on self test at any time using the following CLI command:

```
fips_algvs fips_test_suite post
```

More complete and extensive self tests can be performed by omitting the `post` argument.

The cryptographic module integrity is verified by performing a hash (sha1) on the FIPS object module. The digest must match the expected digest value embedded within the FIPS object module. This integrity check is also performed every time an application enables the FIPS_mode of the cryptographic module.

Next cryptographic algorithms are tested as described in Table 20. The elements not pertinent to the current ST are grayed out. Failure can be artificially induced by specifying an error trigger on the command line. This trigger is defined in parenthesis in the simulated failure description (ex: drbg).

```
fips_algvs fips_test_suite post <error-trigger>
```

Group	Algorithms	Test
DRBG	CTR AES-256-CTR DF CTR AES-256-CTR HASH SHA256 HMAC SHA256 Dual EC P-256 SHA256	Instantiate and generate KAT on each supported DRBG. Failure (drbg) simulated with shorter "additional input" compared to the KAT value.

X9.31 PRNG	keylen=16
	keylen=24
	keylen=32
		n/a

Digest	SHA1 SHA256	Digest KAT. Failure (sha1) simulated with an extra byte that is digested in addition to the KAT value.

Copyright © 2012 Haivision Network Video. All rights reserved. The Haivision logo, Furnace, Mako, Makito, Barracuda, Piranha, Stingray, InStream, Torpedo, Kraken, CoolSign, KulaByte and Hydra are trademarks of Haivision Network Video. Other trademarks in this document are the property of their respective owners. All specifications are subject to change without notice.

Group	Algorithms	Test
HMAC	SHA1 SHA224 SHA256 SHA384 SHA512	HMAC KAT. Failure (hmac) simulated with an extra byte that is HMACed in addition to the KAT value.
CMAC	AES-128-CBC AES-192-CBC AES-256-CBC DES-EDE3-CBC	CMAC KAT. Failure (cmac) simulated with an extra byte that is CMACed in addition to the KAT value. CMAC is not used by the TOE but this test exercises the AES-CBC mode.
Cipher	AES-128-ECB CCM GCM DES-EDE3-ECB	Known key, IV, and plaintext is encrypted and the output ciphertext compared to a known good value. Ciphertext is then decrypted using same key and IV and the result compared to the original plaintext. Failure (aes) simulated with corrupted ciphertext (first byte XORed with 0x1) before decryption.
GCM	AES-256-GCM	n/a
CCM	AES-256-CCM	n/a
XTS	AES-128-XTS AES-256-XTS	n/a
Digital signature	RSA ECDSA P-224 ECDSA K-233 DSA	Known data signed using a known private key. Deterministic RSA (PSS padding, SHA256, 2048 bit key) signature compared to a known good value. The signature is verified using the same data used for the signature. Failure (rsa) simulated with an extra byte that is digested in addition to the known data for signature creation only.
ECDH	P-224	n/a

Table 20: Cryptographic Module Self Test

The health of the hardware-based noise source of the DRBG is measured at startup. If the calculated entropy is out of bounds, a low entropy failure is reported.

Failures of the power-on self test are reported to the system messages (see the CLI `messages` command or the WCI Messages page). The error message is prefixed by “POST:” and is either failure to run the self test or failure of the self test itself.

Copyright © 2012 Haivision Network Video. All rights reserved. The Haivision logo, Furnace, Mako, Makito, Barracuda, Piranha, Stingray, InStream, Torpedo, Kraken, CoolSign, KulaByte and Hydra are trademarks of Haivision Network Video. Other trademarks in this document are the property of their respective owners. All specifications are subject to change without notice.

6.1.7 TOE Access

The TOE presents a warning and consent message before establishing an interactive session with any user role (*Administrator*, *Operator*, or *Guest*) and terminates the session if it remains idle for a configured period of time.

An interactive session is established either via local CLI using the serial port, or remotely via CLI with SSH or a web browser using HTTPS.

The TOE Access function is designed to satisfy the following security functional requirements:

- **FTA_SSL_EXT.1, FTA_SSL.3**: The TOE implements an autologout session policy to terminate inactive interactive local (serial port) and remote sessions (SSH or HTTPS) that requires administrative users to login again.

  The autologout policy is enabled and configured (idle timeout) by *Security Administrators* using the CLI `policy` (session) command or the WCI Policies page.

- **FTA_SSL.4**: The TSF supports the CLI logout command and a WCI Logout menu item to terminate administrative users' own local or remote session.

- **FTA_TAB.1**: The TOE implements a warning and consent message regarding unauthorized use of the TOE that is defined by *Security Administrators*. This message banner is presented before all interactive sessions.

  The banner, a text file, can be uploaded and enabled by *Security Administrators* using the CLI `banner` command or the WCI Banner page.

6.1.8 Trusted Path/Channels

The TSF can be configured to transmit its audit records to a remote audit server. The TSF also supports remote interactive CLI and web interface sessions.

The cryptographic support for the CC evaluated configuration is set with the CLI `policy` (crypto) command or WCI Policies page. Setting the crypto compliance policy to Makito21st (Makito 2.1 Security Target) sets, upon next reboot, the FIPS mode of operation of the cryptographic module, along with other cryptographic restrictions for TLS, SSH, and HTTPS.

The Trusted Path/Channels function is designed to satisfy the following security functional requirements:

- **FTP_ITC.1**: The TSF secures its remote audit server channel using TLS. See the Security Audit section of this chapter (TSS) for details.

- **FTP_TRP.1**: The TSF secures its CLI remote interactive sessions using SSH and its web interface (WCI) sessions using HTTPS. The TOE also supports telnet sessions but this service is disabled by *Security Administrators* as preparative procedures for the CC evaluated configuration.

- **FCS_TLS_EXT.1:** The TSF supports TLS 1.0 (RFC 2246), TLS 1.1 (RFC 4346), and TLS 1.2 (RFC 5246) using OpenSSL 1.0.1c-fips.

Copyright © 2012 Haivision Network Video. All rights reserved. The Haivision logo, Furnace, Mako, Makito, Barracuda, Piranha, Stingray, InStream, Torpedo, Kraken, CoolSign, KulaByte and Hydra are trademarks of Haivision Network Video. Other trademarks in this document are the property of their respective owners. All specifications are subject to change without notice.

For the CC evaluated configuration, the crypto compliance policy is set to Makito21ST (See 15.1.2 Cryptographic Support), which imposes the following settings: the cryptographic module is operated in FIPS mode, SSLv2 and SSLv3 are disabled, and TLS is restricted to the ciphersuites of Table 22.

Crypto Compliance Policy	None	Makito 2.1 Security Target
FIPS mode	No	Yes
SSLv2	No	No
SSLv3	Yes	No
TLSv1.0/1.1/1.2	Yes	Yes
TLS Ciphersuites	Default	See next table

Table 21: TLS Settings

TLS Ciphersuite	OpenSSL setting
TLS_RSA_WITH_AES_128_CBC_SHA	AES128-SHA
TLS_RSA_WITH_AES_256_CBC_SHA	AES256-SHA
TLS_DHE_RSA_WITH_AES_128_CBC_SHA	DHE-RSA-AES128-SHA
TLS_DHE_RSA_WITH_AES_256_CBC_SHA	DHE-RSA-AES256-SHA
TLS_RSA_WITH_AES_128_CBC_SHA256	AES128-SHA256
TLS_RSA_WITH_AES_256_CBC_SHA256	AES256-SHA256
TLS_DHE_RSA_WITH_AES_128_CBC_SHA256	DHE-RSA-AES128-SHA256
TLS_DHE_RSA_WITH_AES_256_CBC_SHA256	DHE-RSA-AES256-SHA256

Table 22: Makito 2.1 Security Target TLS Ciphersuites

TLS is used to secure the web interface (HTTPS server) and the audit server channel (syslog client).

- **FCS_SSH_EXT.1**: The TSF implements SSH v2.0 as specified in RFC 4253 (transport), RFC 4252 (authentication), and RFC 4255 (connection) using OpenSSH 6.0p1 (customized to support FIPS mode) and OpenSSL 1.0.1c-fips operated in FIPS mode.

  Password-based and public key-based authentications are supported. Administrative users can manage their public keys using the CLI `pubkey` command or the WCI My Account page. *Security Administrators* can manage the key of any administrative user with the CLI `account` (pubkey) command or the WCI Accounts page.

  The SSH implementation discards packets greater than 256 Kbytes. It closes the connection when it detects that the 32-bit packet length field of the SSH packet is larger than 256 Kbytes.

Copyright © 2012 Haivision Network Video. All rights reserved. The Haivision logo, Furnace, Mako, Makito, Barracuda, Piranha, Stingray, InStream, Torpedo, Kraken, CoolSign, KulaByte and Hydra are trademarks of Haivision Network Video. Other trademarks in this document are the property of their respective owners. All specifications are subject to change without notice.

For the CC evaluated configuration, the crypto compliance policy is set to `Makito21ST` (See 15.1.2 Cryptographic Support), imposing the SSH setting of the last column of Table 23.

Crypto Compliance Policy	None	Makito 2.1 Security Target
FIPS mode	No	Yes
SSHv1	No	No
SSHv2 DSA key	1024	No
SSHv2 ECDSA key	sha2-nistp256	No
SSHv2 RSA key	2048	2048
SSHv2 Key Exchange	any	diffie-helman-group14-sha1
SSHv2 Ciphers	any	aes128-cbc, aes256-cbc
SSHv2 MACs	any	hmac-sha1

Table 23: SSH Settings

- **FCS_HTTPS_EXT.1**: The TSF implements HTTPS using TLS described earlier.

  The TSF HTTPS implementation authenticates the TOE to the remote client with an X.509 certificate. *System Administrators* manage TOE identity certificates using the CLI `certificate` command or the WCI Certificates page. HTTPS uses the *Security Administrator*-selected identity certificate.

  The TOE does not support unsecured HTTP. It creates a self-signed certificate the first time it boots with the factory default IP address. This self-signed certificate is recreated the first time the TOE boots with a non-factory IP address (to set the certificate Common Name and Subject Alternative Name to the TOE network configuration). *Security Administrators* can generate a Certificate Signing Request and later import the CA-signed certificate matching the private key. *Security Administrators* can also import certificate and its private key.

  The TSF HTTPS implementation does not require client authentication at the TLS level but presents the Web interface logon page for administrative users to authenticate using their name and password.

Copyright © 2012 Haivision Network Video. All rights reserved. The Haivision logo, Furnace, Mako, Makito, Barracuda, Piranha, Stingray, InStream, Torpedo, Kraken, CoolSign, KulaByte and Hydra are trademarks of Haivision Network Video. Other trademarks in this document are the property of their respective owners. All specifications are subject to change without notice.

7. Security Requirements Rationale

7.1.1 Rationale for Security Functional Requirements

The tables below demonstrate the completeness and sufficiency of SFRs that fulfill the objectives of the TOE.

SFRs	Security Objectives							
	O.PROTECTED_COMMUNICATIONS	O.VERIFIABLE_UPDATES	O.SYSTEM_MONITORING	O.DISPLAY_BANNER	O.TOE_ADMINISTRATION	O.RESIDUAL_INFORMATION_CLEARING	O.SESSION_LOCK	O.TSF_SELF_TEST
FAU_GEN.1			X					
FAU_GEN.2			X					
FAU_STG_EXT.1			X					
FCS_CKM.1	X							
FCS_CKM_EXT.4	X							
FCS_COP.1(1)	X							
FCS_COP.1(2)	X	X						
FCS_COP.1(3)	X	X						
FCS_COP.1(4)	X							
FCS_RBG_EXT.1	X							
FCS_TLS_EXT.1	X							
FCS_SSH_EXT.1	X							

Copyright © 2012 Haivision Network Video. All rights reserved. The Haivision logo, Furnace, Mako, Makito, Barracuda, Piranha, Stingray, InStream, Torpedo, Kraken, CoolSign, KulaByte and Hydra are trademarks of Haivision Network Video. Other trademarks in this document are the property of their respective owners. All specifications are subject to change without notice.

SFRs	Security Objectives							
	O.PROTECTED_COMMUNICATIONS	O.VERIFIABLE_UPDATES	O.SYSTEM_MONITORING	O.DISPLAY_BANNER	O.TOE_ADMINISTRATION	O.RESIDUAL_INFORMATION_CLEARING	O.SESSION_LOCK	O.TSF_SELF_TEST
FCS_HTTPS_EXT.1	X							
FDP_RIP.2						X		
FIA_PMG_EXT.1					X			
FIA_UIA_EXT.1					X			
FIA_UAU_EXT.2					X			
FIA_UAU.7					X			
FMT_MTD.1					X			
FMT_SMF.1					X			
FMT_SMR.2					X			
FPT_SKP_EXT.1	X							
FPT_APW_EXT.1					X			
FPT_STM.1			X					
FPT_TUD_EXT.1		X						
FPT_TST_EXT.1								X
FTA_SSL_EXT.1					X		X	
FTA_SSL.3					X		X	
FTA_SSL.4					X		X	
FTA_TAB.1				X				

Copyright © 2012 Haivision Network Video. All rights reserved. The Haivision logo, Furnace, Mako, Makito, Barracuda, Piranha, Stingray, InStream, Torpedo, Kraken, CoolSign, KulaByte and Hydra are trademarks of Haivision Network Video. Other trademarks in this document are the property of their respective owners. All specifications are subject to change without notice.

SFRs	Security Objectives							
	O.PROTECTED_COMMUNICATIONS	O.VERIFIABLE_UPDATES	O.SYSTEM_MONITORING	O.DISPLAY_BANNER	O.TOE_ADMINISTRATION	O.RESIDUAL_INFORMATION_CLEARING	O.SESSION_LOCK	O.TSF_SELF_TEST
FTP_ITC.1	X		X					
FTP_TRP.1	X							

Table 24: Completeness of the Security Functional Requirements

Copyright © 2012 Haivision Network Video. All rights reserved. The Haivision logo, Furnace, Mako, Makito, Barracuda, Piranha, Stingray, InStream, Torpedo, Kraken, CoolSign, KulaByte and Hydra are trademarks of Haivision Network Video. Other trademarks in this document are the property of their respective owners. All specifications are subject to change without notice.

Objective	SFR	Rationale
O.PROTECTED_COMMUNICATIONS The TOE will provide protected communication channels for administrative users, other parts of a distributed TOE, and authorized IT entities.	FPT_TRP.1: Trusted Path FCS_SSH_EXT.1: Explicit: SSH FCS_HTTPS_EXT.1: Explicit: HTTPS FPT_ITC.1: Inter-TSF Trusted Channel FAU_GEN_EXT.1: External Audit Trail Storage FCS_CKM.1: Cryptographic Key Generation (for asymmetric keys) FCS_CKM_EXT.4: Cryptographic Key Zeroization FCS_COP.1(1): Cryptographic Operation (for data encryption/decryption) FCS_COP.1(2): Cryptographic Operation (for cryptographic signature) FCS_COP.1(3): Cryptographic Operation (for cryptographic hashing) FCS_COP.1(4): Cryptographic Operation (for keyed-hash message authentication) FCS_RBG_EXT.1: Extended: Cryptographic Operation (Random Bit Generation) FPT_SKP_EXT.1: Protection of TSF Data (for reading of all symmetric keys)	FCS_TRP.1 and its descendent requirements protect the communication channels for administrative users using Trusted Path for management interfaces such as the CLI (FCS_SSH_EXT.1) and the web interface (FCS_HTTPS_EXT.1). FCS_ITC.1 protects the communication using TLS (FCS_TLS_EXT.1) with the authorized IT entities such as the External Audit Trail Storage (FAU_GEN_EXT.1). The other FCS family SFRs fulfill the cryptographic services and dependencies of the above requirements. All remote management interfaces (CLI, web interface) and all remote IT entities (Audit server) communications are covered by these requirements.
O.VERIFIABLE_UPDATES The TOE will provide the capability to help ensure that any updates to the TOE can be verified by the *Security Administrator* to be unaltered and (optionally) from a trusted source.	FPT_TUD_EXT.1: Extended: Trusted Update FCS_COP.1(2): Cryptographic Signature FCS_COP.1(3): Cryptographic hashing	FPT_TUD_EXT.1 ensures the *Security Administrator* can validate a firmware upgrade integrity from its hash (FCS_COP.1(3)) and confirm its origin from its digital signature (FCS_COP.1(2)).
O.SYSTEM_MONITORING The TOE will provide the capability to generate audit data and send those data to an external IT entity.	FAU_GEN.1: Audit Data Generation FAU_GEN.2: User Identity Association FAU_STG_EXT.1: External Audit Trail Storage FPT_ITC.1: Inter-TSF Trusted Channel FPT_STM.1: Reliable Time Stamps	FAU_GEN.1 defines the audit data to generate with reliable time stamp (FPT_STM.1) and associated with user identity when available (FAU_GEN.2). Audit data is sent to an external audit server (FAU_STG_EXT.1) over a trusted channel (FTP_ITC.1). The *Security Administrators* are notified when communication with the external audit server is lost.

Copyright © 2012 Haivision Network Video. All rights reserved. The Haivision logo, Furnace, Mako, Makito, Barracuda, Piranha, Stingray, InStream, Torpedo, Kraken, CoolSign, KulaByte and Hydra are trademarks of Haivision Network Video. Other trademarks in this document are the property of their respective owners. All specifications are subject to change without notice.

Objective	SFR	Rationale
O.DISPLAY_BANNER The TOE will display an advisory warning regarding use of the TOE.	FTA_TAB.1: Default TOE Access Banners	FTA_TAB.1 implements the O.DISPLAY_BANNER directly.
O.TOE_ADMINISTRATION The TOE will provide mechanisms to ensure that only administrators are able to log in and configure the TOE, and provide protections for logged-in administrators.	FMT_MTD.1: Management of TSF Data (for general TSF data) FMT_SMF.1: Specification of Management Functions FMT_SMR.2: Restrictions on Security Roles FIA_PMG_EXT.1: Password Management FIA_UIA_EXT.1: User Identification and Authentication FIA_UAU_EXT.2: Extended: Password-based Authentication Mechanism FIA_UAU.7: Protected Authentication Feedback FPT_APW_EXT.1: Protection of Administrator Passwords FTA_SSL_EXT.1: TSF-initiated Session Locking FTA_SSL.3: TSF-initiated Termination FTA_SSL.4: User-initiated Termination	FMT_MTD.1 specifies that only the *Security Administrator* can manage the TSF data and perform the management functions defined in FMT_SMF.1. FMT_SMR.2 specifies that the *Security Administrator* is the only security role. The FIA family defines the password-based identification and authentication requirements and FPT_APW_EXT.1 requires the protection of the authentication data. FTA_SSL_EXT.1 ensures unattended (inactive) sessions are closed and FTA_SSL.3 and FTA_SSL.4 ensure closed session requires user re- authentication to re-open.
O.RESIDUAL_INFORMATION_CLEARING The TOE will ensure that any data contained in a protected resource is not available when the resource is reallocated.	FDP_RIP.2: Full Residual Information Protection	FDP_RIP.2 requires resource zeroization at allocation time so the media content (user data) cannot leak outside the process streaming process through dynamic memory re-allocation and fulfills O.RESIDUAL_INFORMATION_CLEARING.
O.SESSION_LOCK The TOE shall provide mechanisms that mitigate the risk of unattended sessions being hijacked.	FTA_SSL_EXT.1: TSF-initiated Session Locking FTA_SSL.3: TSF-initiated Termination FTA_SSL.4: User-initiated Termination	FTA_SSL_EXT.1 ensures unattended (inactive) sessions are closed and FTA_SSL.3 and FTA_SSL.4 ensure closed session requires user re- authentication to re-open.

Copyright © 2012 Haivision Network Video. All rights reserved. The Haivision logo, Furnace, Mako, Makito, Barracuda, Piranha, Stingray, InStream, Torpedo, Kraken, CoolSign, KulaByte and Hydra are trademarks of Haivision Network Video. Other trademarks in this document are the property of their respective owners. All specifications are subject to change without notice.

Objective	SFR	Rationale
O.TSF_SELF_TEST The TOE will provide the capability to test some subset of its security functionality to ensure it is operating properly.	FPT_TST_EXT.1: TSF Testing	FPT_TST_EXT.1 implements the O.TSF_SELF_TEST directly.

Table 25: Sufficiency of the Security Functional Requirements

Copyright © 2012 Haivision Network Video. All rights reserved. The Haivision logo, Furnace, Mako, Makito, Barracuda, Piranha, Stingray, InStream, Torpedo, Kraken, CoolSign, KulaByte and Hydra are trademarks of Haivision Network Video. Other trademarks in this document are the property of their respective owners. All specifications are subject to change without notice.