

ALTEON SECURITY TARGET

Author: Yariv Katz
October 06, 2022

Version Control

Version	Comments	Date
1.0	First document release	August 2021
1.1	<p>Fixed inconsistent identification of the TOE in section 2.2.2 and 2.3.</p> <p>Added missing supplementary guide to the documental delivery in section 2.3.1.1.</p> <p>Fixed outdated version of CC standard reference in section 10.</p> <p>Reworded the T.PASSWORD_CRACKING threat to better suit the security problem in section 4.2.1 and the rationale in section 7.4.1.</p> <p>Fixed an erroneous “and” operation in section 6.1.1.2.1.</p> <p>Fixed incorrect reference to ALC_CMS.2 and ATE_IND.2 SARs in section 7.3.</p> <p>Removed invalid assignment of RFC 4253 to FCS_CKM.2 in section 7.2.2.3.</p> <p>Fixed invalid operation of FTP_ITC.1 in section 7.2.8.1.</p> <p>Fixed invalid operations of FTP_TRP.1 in section 7.2.8.2.</p> <p>Fixed invalid operations and reproduction of FCS_TLS.1 in section 7.2.2.6.</p> <p>Fixed errata in FCS_CKM.1/RSA and FCS_CKM.1/EC</p> <p>Added application note for FMT_MSA.3 in section 7.2.5.2.</p> <p>Added missing component of the O.AUDIT security objective in section 7.4.1.</p> <p>Removed invalid component of O.TRUSTED_CHANNELS security objective rationale in section 7.4.1.</p> <p>Expanded details regarding audit accessibility of user roles in section 8.1.</p> <p>Reworded part of section 6.1.1.1 to avoid conflict with the formal role definition.</p>	February 2022

Version	Comments	Date
	<p>Updated section 7.4.1.1 to more accurately describe some dependencies of SFRs being fulfilled by hierarchical components.</p> <p>Added table and figure titles.</p> <p>Updated acronyms table.</p>	
1.2	<p>Changes introduced addressing feedback:</p> <ul style="list-style-type: none"> - Added a new section 2.2 where the general product descriptions is included, leaving the TOE-specific sections free of any reference to functionality outside of the evaluation scope. - Added section 2.3.3.2 to indicate the optional syslog server in the non-TOE component section. - Expanded description of section 2.3.3.1 to better indicate that the TOE has multiple images for the different virtualization platforms. - Minor re-wording when referring to figure 1 in section 2.4. - Changed description of section 2.4.1 to better indicate that the Help documentation is part of the TOE and not a separate guidance document. - Changed section 2.4.1.2 to more accurately indicate the use for each software image delivered as the TOE. - Changed section 2.4.1.3 to reference the Alteon Common Criteria Guide when detailing the evaluated configuration. - Changed naming of FCS_HTS.1 and FCS_TLS.1 to be more consistent throughout their definition and usage. - Fixed an inconsistent style being applied to the FIA_AFL.1.2 component. - Changed sections 8.2 and 8.8 to remove any ambiguity when mentioning the secure communication channels. 	March 15 th 2022
1.3	<p>Changes introduced addressing feedback:</p> <ul style="list-style-type: none"> - Section 2 has been extensively re-written to provide a different approach on how describe the TOE. The TOE is now Alteon and it is an ADC, but the TSF is the subset of SLB features together with the SSL offloading. 	March 30 th 2022

Version	Comments	Date
	<ul style="list-style-type: none"> - Added new subsections to the physical scope description in section 2.4.1.2 to include a more details regarding how the Alteon images are segmented based on the target platform. 	
1.4	Changed the version to align a new release.	April 28 th 2022
1.5	<p>Changes introduced addressing feedback:</p> <ul style="list-style-type: none"> - Moved the Optional Syslog section to 2.4.2.9.1 to more accurately represent the optional capabilities to export audit logs to syslog servers as non-TSF. - Modified section 2.4.1.3 to remove the incorrect inclusion of the syslog as TSF. - Removed syslog from section 8.1 since it is not part of the TSF. - Removed miss rate mention from section 2.3 since it is not part of the FDP_IFF.1 SFR. - Modified section 2.4.1 to clarify that the help webpages are not actual standalone documentation, but rather part of the product itself. - Modified section 2.4.1.1 to clarify how the Common Criteria specific documentation is delivered. - Removed the list of supported hardware appliances from section 2.4.1.2.1 since it is a duplicate of the one defined in section 2.4.1. - Modified subsections of 2.4.1.2 to more clearly state the need to download the TOE images as part of the delivery. - Removed the unsupported LDAP mentioned in section 2.4.1.3. - Modified section 4.2.1 to more accurately represent the danger of using the TSF as an exfiltration mechanism. - Removed application note from 7.2.5.3 and included all of the management functions more explicitly in the SFR. - Added new iteration of FCS_TLS.1 to split the implementation of the secure channels of the Web Management (HTTPS) and the data paths(Egress and Ingress Port). Sections 7.2.2, 7.4.1 and 8.2 have been modified accordingly. 	August 3 th 2022

Version	Comments	Date
	<ul style="list-style-type: none"> - Modified section 8.5 to more clearly state the reason for listing all available roles, even if they are not relevant to the TSF. - Added missing rationale to the mapping between O.TRAFFIC_FLOW and FMT_SMF.1 in section 7.4.1. - Modified sections 4.3.2, 5.1.3, 5.3.2 and 7.4.1 to remove an invalid statement regarding log review. - Updated section 10 to include all of the missing references to RFCs. - Changed figure 1 to remove the VM component, since the VA can be considered a standalone unit on top of the virtualization platform. - Updated section 6.1.1 Class FCS: Cryptographic support - Document Format 	
1.6	<p>Changes introduced:</p> <ul style="list-style-type: none"> - Removed duplicated information. - Removed disclosure section. - Updated TSS section - Updated Section 6. Extended Component Definition - Updated Minor Change in Section 8.1.1 Security Audit - Updated Minor Change in Section 7.2. Security Functional Requirement 	August 10, 2022
1.7	<p>Changes introduced:</p> <ul style="list-style-type: none"> - Updated Section 2.4.1.4 TOE DELIVERY. 	September 21, 2022
1.8	<p>Changes introduced:</p> <ul style="list-style-type: none"> - Updated Interfaces Name. 	October 06, 2022



Table of Contents

1.	Scope of the Document	10
2.	Introduction	11
2.1	Identification	11
2.2	Product Introduction	11
2.3	TOE Overview	12
2.3.1	TOE Usage	13
2.3.2	TOE Type	14
2.3.3	Functionality Outside of the Scope	14
2.3.4	Non TOE Hardware and Software	14
2.4	TOE Description	15
2.4.1	Physical Scope	16
2.4.2	Logical Scope	25
3.	Conformance Claims	28
3.1	Common Criteria Conformance Claim	28
3.2	Protection Profile Conformance Claim	28
3.3	Package Claim	28
3.4	Conformance Rationale	28
4.	Security Problem Definition	29
4.1	TOE Assets	29
4.1.1	AS.CONFIGURATION	29
4.1.2	AS.LOGS	29
4.1.3	AS.CREDENTIALS	29
4.1.4	AS.DATA	29
4.1.5	AS.CORE_FUNCTIONALITY	29
4.2	Threats	29
4.2.1	T.PASSWORD_CRACKING	29



4.2.2	T.UNDETECTED_ACTIVITIES	29
4.2.3	T.WEAK_CRYPTOGRAPHY	30
4.2.4	T.WEAK_ENDPOINTS.....	30
4.2.5	T.UNBALANCED_LOAD.....	30
4.3	Organizational Policies	30
4.3.1	OSP.ROLES.....	30
4.3.2	OSP.LOGS	30
4.3.3	OSP.ACCOUNTABILITY.....	30
4.3.4	OSP.TRUSTED_ADMINISTRATORS.....	31
4.4	Assumptions	31
4.4.1	A.PHYSICAL_PROTECTION.....	31
4.4.2	A.MANAGEMENT_SEPARATION	31
4.4.3	A.NO_EVIL	31
4.4.4	A.LIMITED_FUNCTIONALITY.....	31
5.	Security Objectives	32
5.1	Security Objectives for the TOE.....	32
5.1.1	O.ACCESS.....	32
5.1.2	O.ADMINISTRATION.....	32
5.1.3	O.AUDIT.....	32
5.1.4	O.TRUSTED_CHANNELS.....	32
5.1.5	O.TRAFFIC_FLOW	33
5.2	Security Objectives for the Operational Environment.....	33
5.2.1	OE.TRUSTED_ADMINIS.....	33
5.2.2	OE.PHYSICAL_SECURITY	33
5.2.3	OE.NO_GENERAL_PURPOSE	33
5.3	Security Objectives Rationale.....	33
5.3.1	Threats	34
5.3.2	Organizational Security Policies	35



5.3.3	Assumptions.....	35
6.	Extended Component Definition	37
6.1	Extended Security Functional Requirements	37
6.1.1	Class FCS: Cryptographic support	37
7.	Security Requirements	42
7.1	Conventions.....	42
7.2	Security Functional Requirements	42
7.2.1	Security Audit (FAU).....	43
7.2.2	Cryptographic support (FCS)	44
7.2.3	User data protection (FDP)	48
7.2.4	Identification and Authentication (FIA)	50
7.2.5	Security Management (FMT)	50
7.2.6	Protection of the TSF (FPT)	52
7.2.7	TOE Access (FTA)	53
7.2.8	Trusted Path (FTP).....	53
7.3	Assurance Security Requirements.....	54
7.4	Rationale for the Security Requirements	55
7.4.1	Rationale for the Security Functional Requirements.....	55
7.4.2	Rationale for the Security Assurance Requirements	60
8.	TOE Summary Specification.....	61
8.1	Description on how toe meets each sFR	61
8.1.1	Security Audit.....	61
8.1.2	Cryptographic Support.....	61
8.1.3	User Data Protection.....	61
8.1.4	Identification and Authentication.....	62
8.1.5	Security Management.....	62
8.1.6	Protection of the TSF	64
8.1.7	TOE Access	64



8.1.8	Trusted Path/Channels	64
8.2	Functionality Outside of the Scope	64
9.	Acronyms	66
10.	References	67



1. Scope of the Document

The aim of this document is to define the scope of the evaluation in terms of the assumptions made, the intended environment for the Target of Evaluation (TOE), the Information Technology (IT) security functional and assurance requirements to be met, and the level of confidence (evaluation assurance level) to which it is asserted that the TOE satisfies its IT security requirements.

2. Introduction

2.1 IDENTIFICATION

Document Identifier:	Alteon Security Target
Document Version:	1.8
TOE Name:	Alteon
TOE Version:	32.6.3.50
TOE Type:	Load Balancer
Created By:	Yariv Katz
Publication Date:	October 06, 2022

TABLE 1 - TOE IDENTIFICATION

2.2 PRODUCT INTRODUCTION

Alteon is Radware's next-generation Application Delivery Controller (ADC) and the only network load balancer that guarantees application Service Level Agreement (SLA). It provides advanced, end-to-end local and global load balancing capabilities for all Web, cloud and mobile-based applications.

Alteon combines best-of-breed application delivery capabilities, market-leading SSL performance that supports all of the latest encryption protocols, and advanced services to companies with ongoing application lifecycle management challenges that impact the performance of web applications (such as heavier, more complex web content); mobility, and the migration to the cloud.

Alteon is designed to provide best-in-class ADC capabilities with:

Server Load Balancing

The core function of Alteon is to provide comprehensive load balancing and traffic shaping capabilities needed to meet any customer need.

Application SLA Assurance

Load balancing complete with fault isolation, vADC per application and service, and the ability to scale up or scale out while maintaining performance with ADC-VX¹, Alteon Virtual Appliance (VA), Alteon VA for NFV and Alteon VA for cloud environment form factors.

¹ ADC-VX is Radware's ADC-focused hypervisor design to run multiple vADC instances on dedicated ADC hardware.

Web Performance Optimization

Accelerated web page performance for any end-user device and any browser up to 40% with FastView web performance optimization.

SSL Offloading

SSL termination, inspection and acceleration with the flexibility of security policies and accelerated processing via hardware on selected platforms.

Application SLA Monitoring

Real-time monitoring, proactive SLA management and assurance with agent-less application performance monitoring (APM).

Application Firewall

Layer 7 security with AppWall for detection and prevention of application level attacks such as SQL injections, cookie tampering, etc.

Layered Security Architecture

Additional protection for applications and infrastructure against cyber-attacks, with accurate attack detection and DoS signaling, in the perimeter or the cloud via Radware's Attack Mitigation System (AMS).

Management Capabilities

Alteon supports local or remote management via serial, SSH and its own web-based Web Management interface (HTTPS). Furthermore, Alteon can be also integrated with Radware's APSolute Vision for a centralized organization.

2.3 TOE OVERVIEW

The TOE is the Alteon version 32.6.3.50 series of products, with the TSF covering the core load balancing capabilities together with the SSL Offloading and part of the management capabilities. The TOE, thus, acts as a load balancer which redirects service request in a balanced way to multiple providing servers. As such, from hence forward the TOE may be referred as an ADC or as a load balancer interchangeably. Additionally, the TOE provides the following major security features:

- Security Audit
- Cryptographic Support
- User Data Protection
- Identification and Authentication
- Security Management

- Protection of the TSF
- TOE Access
- Trusted Path/Channels

In order to guarantee proper load balancing, the TOE sits in between the servers and their clients. The TOE provides extensive configuration options for its core load balancing functionality, allowing users to model servers and virtual services down to very fine grained parameters such as:

- Server bandwidth and throughput
- Server groups load balancing policies based on
 - Latency
 - Bandwidth
 - Client data (IP, port)
 - Numbers of connections
- Virtual services session management
- Virtual services based bandwidth management

Furthermore, the TOE provides highly configurable SSL offloading capabilities which guarantee protection of the data transmitted between client and TOE, as well as between the TOE and the back end servers via:


- Virtual service certificate management
- Cipher suite configuration
- Client authentication policies
- Pass-through information
- Traffic matching (URL, IP, etc.)

And a large set of other complementary functionalities ranging from TOE management to supporting various technologies for complex deployments (VLANs, BGP, etc.):

- User and role management
- Network configuration

2.3.1 TOE USAGE

The TOE, at its most basic, is used as a reverse proxy which is installed between service-providing servers and service-consuming users. It is setup as just another network entity by which traffic flows into and is re-routed as per the administrator configuration.



The TOE active users are the administrators, who configure the traffic shaping capabilities via the Web Management Interface (HTTPS); while the passive users are the service consumers, whose service request are routed transparently to and from the servers.

2.3.2 TOE TYPE

The TOE is an application delivery controller with its core function been a load balancer capable of managing and shaping network traffic to better suit the needs of clients.

2.3.3 FUNCTIONALITY OUTSIDE OF THE SCOPE

The following TOE functionality falls outside of the scope of the evaluation and will not be evaluated:

- Server health checks
- Application SLA Assurance implementing the high availability and clustering capabilities.
- Web Performance Optimization implementing optimization technologies with FastView.
- Application SLA Monitoring implementing advanced monitoring and application performance metrics.
- Application Firewall implementing an application layer firewall capabilities with AppWall.
- Layered Security Architecture implementing additional security features.
- Review Logs Stored in the TOE

2.3.3.1 OPTIONAL SYSLOG

The TOE has the capability to export the audit events to external syslog servers. This functionality is optional and in order to use it the administrator must have a syslog server on the management network. The syslog support is not part of the TSF, and its usage does not impact the internal storage capabilities of the TOE.

The TOE can be configured to use both, the BSD (RFC3164) or the IETF (RFC5424) formats. And additionally, it can be configured to use syslog on top of TLS, thus providing support for the different syslog server configurations.

Recommendations are included in the Alteon Common Criteria Guide.

2.3.4 NON TOE HARDWARE AND SOFTWARE

The following components are required for operation of the TOE in CC-evaluated configuration.

2.3.4.1 UNDERLYING PLATFORM

The TOE is deployed on physical appliances or on virtual appliances, both of which are outside of the scope of the evaluation.

For bare-metal installations, at least one appliances from the following line is required:

- Alteon 6420 S
- Alteon 8420 S
- Alteon 8820 S
- Alteon 7220 S
- Alteon 7612 S
- Alteon 9800
- Alteon D-5208
- Alteon D-5424 S
- Alteon D-5820 S

For virtual appliances (VA) installations, the following minimum requirements apply:

- vCPU: 1
- RAM: 2GB
- Disk space: 7GB
- Virtualization Platform:
 - VMWare ESXi
 - KVM
 - Xen
 - KVM (OpenStack)

The VAs is built specifically for specific virtualization platform, for example OVA files are used in VMWare ESXi platform while the image for the KVM platform is an qcow2 or tgz file. For more details on supported hardware and their configuration see the Alteon VA Installation Guide.

2.3.4.2 WEB BROWSER

In order to access the TOE via Web Management Interface (HTTPS) the following web browser must be used:

- Chrome
- Firefox
- MS Edge

2.4 TOE DESCRIPTION

The TOE is a self-contained ADC solution (**Alteon 32.6.3.50**) running on top of a hardware appliance or a virtualized one. The TSF is composed of the network traffic shaping capabilities, by being able



to balance requests made by clients to services being implemented in multiple back end servers; the SSL offloading capabilities, used for decrypting and accessing application level data; and a subset of the management capabilities, used to manage user access control to the TOE configuration.

As stated before, the TOE is pure software solution that can be deployed in a physical or virtualized platform. This will affect the network throughput processed by the TOE (speed or number of ports), but it will not affect the available functionality in any way. Nor will it change the way the TOE is used or accessed. Additionally, for each type of deployment (Virtualized Platform, Alteon Hardware Appliance) the TOE can be deployed in different modes:

ALTEON HARDWARE APPLIANCE	VIRTUALIZED PLATFORM
<p>Standalone deployment mode: The standalone ADC is the most basic form of deployment in which Alteon is installed on top of the hardware appliances and provides a single instance of the TOE.</p> <p>The Alteon image used for this mode is a package (.IMG) containing all of the necessary applications for upgrading the form factors, including the standalone ADC and vADC.</p>	<p>VA deployment mode: The VAs are instances of Alteon packaged as virtual appliances that run on top of server virtualization infrastructure. Therefore, these images can be understood as the virtual machine equivalent to the standalone ADC.</p> <p>The Alteon image used for this mode is a custom package (.OVA, TGZ, or QCOW2) containing all of the necessary applications for installing the form factors VA.</p>
<p>ADC-VX (vADC) deployment mode: The virtual ADC (vADC) form factor is an evolution of the standalone ADC where the functionality is segmented in two parts: a resource management hypervisor ADC-VX; and a number of virtual Alteon instances (vADC).</p> <p>The Alteon image used for this mode are a packages (.IMG) for each part the ADC and the hypervise ADC-VX containing all of the necessary applications for upgrading the form factor vADC</p>	

TABLE 2 – ALTEON DEPLOYMENT MODES

2.4.1 PHYSICAL SCOPE

The TOE consist of a Software **Alteon 32.6.3.50** deployed in a Virtualized Platform or Alteon Hardware Appliance.

2.4.1.1 VIRTUAL APPLIANCES

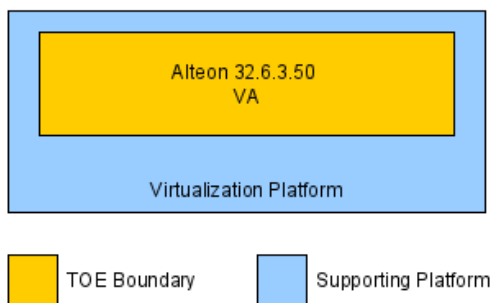


FIGURE 1 - PHYSICAL SCOPE FOR VIRTUAL APPLIANCE

The virtual appliances (VA) correspond to images used to deploy virtual machines containing the Alteon software. The VAs always come as a complete singular Alteon instance and therefore, only one image is provided for each supported platform.

#	File Name	Virtualization Platform	SHA-256
1	AlteonOS-32.6.3.50_rls_74.ova	VMWare VA	d8a9b0fd1228c5ca65fe9d4bad7e0eff781a81942652a822eed5b9005bea0a33
2	AlteonOS-32.6.3.50_rls_74_xen.tgz	Xen VA	fcfd85f91a51e9f67efdf2e640b166a391f34b28a0ae9275db5f4dd43e79ea93
3	AlteonOS-32.6.3.50_rls_74.qcow2	KVM VA (OpenStack)	576aeb728a671b21a20d4a13c35a7359be785576e738ea090ce94d9abf863d2b
4	AlteonOS-32.6.3.50_rls_74_kvm.tgz	KVM VA	6159fc304fc3c909e10036a7847e7f1df94aea2a6d1b094d7e02fa174fd376eb

TABLE 3 - VIRTUAL APPLIANCES IMAGES

- ➔ Image 1 is for VMWare deployments in the OVA format.
- ➔ Image 2 is for Xen deployments and is a compressed package (TGZ).
- ➔ Image 3 is for KVM for cloud environment (Openstack) in QCOW2 format.
- ➔ Image 4 is for KVM deployments and is a compressed package (TGZ).

2.4.1.2 PHYSICAL APPLIANCES

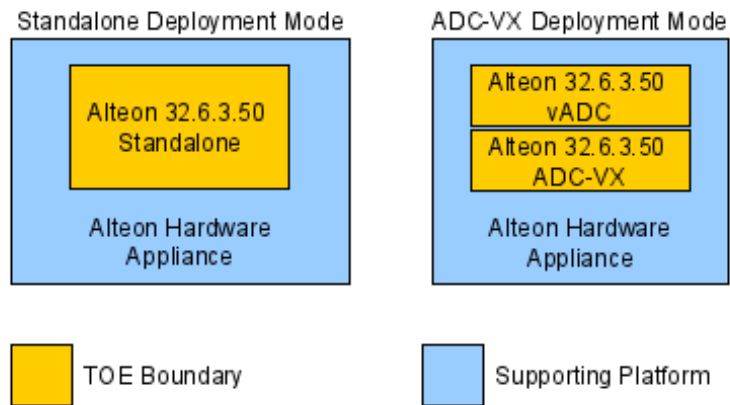


FIGURE 2 - PHYSICAL SCOPE HARDWARE APPLIANCE

The supported physical appliances correspond to, as listed in **2.3.4.1 Underlying Platform**, the Alteon Hardware products.

All these physical appliances don't include the correct version of the TOE hence when the appliance is received, the end user must perform an upgrade process in order to upgrade the TOE to its correct version. Radware maintains a single code base where all of the product features (TSF included) are implemented. The code base is then compiled and packaged specifically for each of the supported underlying platforms, resulting in multiple images. Thus, any change to the code base is observable and applicable to all platforms, guaranteeing the complete equivalency at the functional and security level.

Since the Alteon image for standalone deployment mode contains all of the necessary application for upgrading the form factors ADC and ADC-VX, the following table contains a full list of images that are provided in the IMG format for both deployment modes (Standalone and ADC-VX) and can be used to upgrade Alteon series of products. Additionally, the following table define for each type of Alteon Hardware its corresponding image in order to be upgraded.

#	File Name	Alteon Hardware Appliance	SHA-256
1	AlteonOS-32.6.3.50-5k.6k.8k_rls_74_qat.img	Alteon 6420 S Alteon 8420 S Alteon 8820 S	acba32461f80d422edad451d02972cd38ad4dca0ff95663a796a94d6ea03247
2	AlteonOS-32.6.3.50-DPDK_rls_74.img	Alteon 7220 S Alteon 7612 S Alteon 9800 Alteon D-5208 Alteon D-5424 S Alteon D-5820 S	ef41036bf3cd0d9ce2c12d69afaf17282d50dbf5b53f4ba3ff9bc2a3cebacca2

TABLE 4 - PHYSICAL APPLIANCES IMAGES

2.4.1.3 TOE GUIDANCE

The main documentation that is provided as part of the TOE delivery is:

Alteon Common Criteria Guide, Version 1.7, Hash: e1f3087834580a42b7eb9ca924e9c815e900167a428eeff6682b50428335223e

Additionally, the following complementary documentation is also provided as part of the TOE delivery:

#	Document Name	Document ID	SHA-256
1	Alteon CLI Application Guide	RDWR-ALOS-V3263_CLIAG2012	f3bdf9990c6ddcd0f00da155fc148c15eb1f8d543b21c338e0ec77ee5e1ec70f
2	Alteon Getting Started Guide	RDWR-ALOS-V3263_WBMGS2012	b1e97e8f7cff67c149434abb3f282172d23a1ee01366cb48ecaf1245b3b3cef2
3	Alteon WBM Application Guide	RDWR-ALOS-V3263_WBMAG2012	a3a1b3612cb458ccd7e4438cc3dd5fd9129ee063861ab5916bd14df42915bd90
4	Alteon VA Installation and Maintenance Guide	RDWR-ALOS-V3263_VA_IG2012	fa8392f97cc038bc9eeb89b4c324224af0319552511fa0c1bf488d7492174709
5	Alteon Installation and Maintenance Guide	RDWR-ALOS-V3263_IG2012	0dec82b544be6a63c07457d65259e9ba0cd1feb3e427e1f4741ed412ddf6e1cc

TABLE 5 – TOE GUIDANCES

The listed documentation can be found in PDF format via Radware website. Furthermore, the TOE includes, via its Web Management Interface (HTTPS), complementary information describing what each parameter on the currently accessing interface is used and what values are acceptable. This Alteon Help information is delivered as part of the TOE and can be accessed through the Web Management Interface (HTTPS) by clicking on the “?” button.

2.4.1.4 TOE DELIVERY

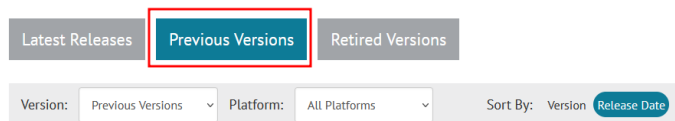
The TOE is a software solution that is provided digitally via Radware web portal. This software can be delivered as follow:

2.4.1.4.1 DELIVERY FOR VIRTUAL APPLIANCES

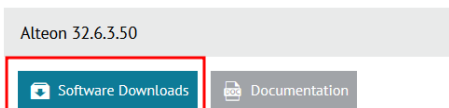
For virtualized platforms the TOE is distributed in different digital formats to accommodate the different virtualization platforms, but all of them can be referred as virtual appliances (VA).

In order to download the image, the end users must purchase the virtual appliance (VA) and the end users will have to register to <https://portals.radware.com/Not-Logged-In/Combined-Registration-Form/> using serial number of the purchased product in order to obtain the credentials to web portal <https://portals.radware.com>. The end users will have to go to the following section <https://portals.radware.com/Customer/Home/Downloads/Application-Delivery-Load-Balancing/> and perform the following steps:

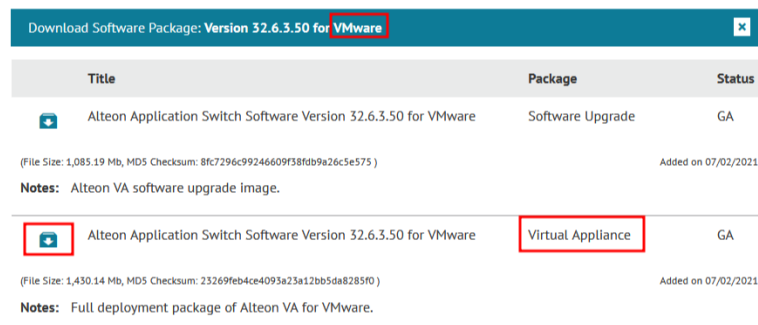
- a) Scroll down to the bottom page and click on the Previous Version button.



- b) Search the version of the TOE, click on it, then click on the Software Download button.



- c) Search the virtual platform, click on it and download the image used for Virtual Appliance. For example:



- d) Validate the integrity with the SHA-256 value defined in **2.4.1.1. Virtual Appliance**. The process for validating the image requires the usage of any software tool capable of calculating the SHA-256 of a given file. For example, the 7-Zip compression/decompression tool includes the capabilities of generating checksum values (hashes). The end user must then, provide the downloaded image (.ova, tgz, or qcow2) to the tool and wait for the generated hash value. Once obtained, the end user will compare the value with the SHA-256

values and determined if they are the same. If the values are identical, then the downloaded image has been properly received and the end user may proceed to perform the installation process. Otherwise, the end user must discard the image and contact Radware technical support via Radware Web Portal <https://support.radware.com> for support in obtaining the correct image.

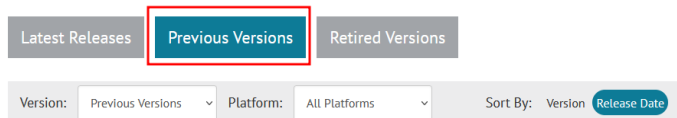
- e) Finally, the end users will have to install the image in the virtualized platform selected.

2.4.1.4.2 DELIVERY FOR PHYSICAL APPLIANCES

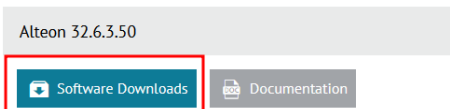
When the TOE is deployed with physical appliances, the developer or the reseller will ship the physical appliance to the end customer by courier. These physical appliances don't come with the correct version of the TOE, hence, in order to provide end to end assurance, once purchased, the end users must update it to the correct version TOE.

The end users will have to register to <https://portals.radware.com/Not-Logged-In/Combined-Registration-Form/> using MAC or serial number of the purchased product in order to obtain the credentials to web portal <https://portals.radware.com>. The end users will have to go to the following section <https://portals.radware.com/Customr/Home/Downloads/Application-Delivery-Load-Balancing/> and perform the following steps:

- a) Scroll down to the bottom page and click on Previous Version button.



- b) Search the version of the TOE, click on it, then click on Software Download button.



- c) Search the physical platform, click on it and download the image used for Software upgrade. For example:

Download Software Package: Version 32.6.3.50 for Alteon 7612 S

Title	Package	Status
Alteon Application Switch Software Version 32.6.3.50 for 5208, 5208 S, D-5424 S/SL, D-5820 S/SL, 7612 S/SL, 7220 S/SL, 9800, 9800 S/SL <small>(File Size: 2,402.44 Mb, MD5 Checksum: c463030a161c53b45e61e518b6f06702)</small>	Recovery File	GA
Alteon Application Switch Software Version 32.6.3.50 for 5208, 5208 S, D-5424 S/SL, D-5820 S/SL, 7612 S/SL, 7220 S/SL, 9800, 9800 S/SL <small>(File Size: 2,346.45 Mb, MD5 Checksum: b84f73db22bc47096213d54e69a69148)</small>	Software Upgrade	GA

Notes: Recovery image

Notes: Combined image for one-step upgrade of both ADC-VX and vADC instances . This image should only be used for upgrade from version 31.0.13.0, 32.2.5.0, 32.4.3.0 or 32.6.1.0 or higher and it should NOT be used for upgrade from versions lower than that. This image can also be used to upgrade Alteon standalone, which later can be transformed to ADC-VX mode.

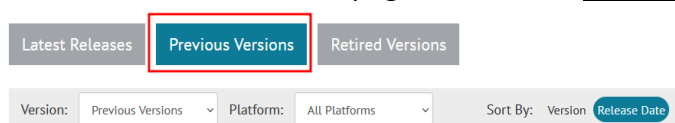
- d) Validate the integrity with the SHA-256 value defined in **2.4.1.2. Physical Appliance**. The process for validating the image requires the usage of any software tool capable of calculating the SHA-256 of a given file. For example, the 7-Zip compression/decompression tool includes the capabilities of generating checksum values (hashes). The end user must then, provide the downloaded image (.img) to the tool and wait for the generated hash value. Once obtained, the end user will compare the value with the SHA-256 values and determined if they are the same. If the values are identical, then the downloaded image has been properly received and the end user may proceed to perform the installation process. Otherwise, the end user must discard the image and contact Radware technical support via Radware Web Portal <https://support.radware.com> for support in obtaining the correct image.
- e) Finally, the end users will have to upgrade the physical platform selected.

Note: The link used to download the image of hardware appliance D-5208 is the link labelled as Alteon 5208 or Alteon 5208_S

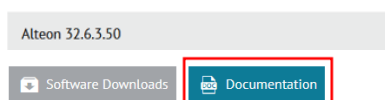
2.4.1.4.3 DELIVERY FOR DOCUMENTATION

In order to get the documentation, the end users must purchase a Virtual Appliance or a Physical Appliance. Then, the end users will have to register to <https://portals.radware.com/Not-Logged-In/Combined-Registration-Form/> using MAC or serial number of the purchased product in order to obtain the credentials to web portal <https://portals.radware.com>. The end users will have to go to the following section <https://portals.radware.com/Customr/Home/Downloads/Application-Delivery-Load-Balancing/> in order to get the complementary documentation and perform the following steps:

- a) Scroll down to the bottom page and click on Previous Version button.



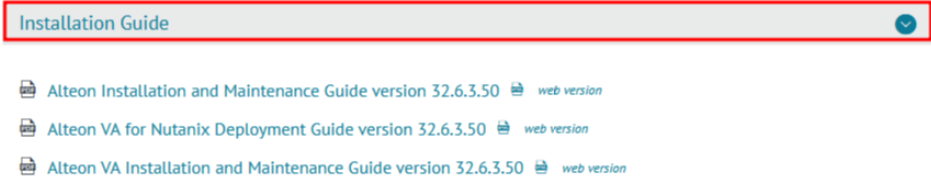
- b) Search the version of the TOE, click on it, then click on the Documentation button.



- c) Click on the User Guide section and download the user guides.



d) Click on the Installation Guide section and select the download the installation guides.



e) Validate the integrity with the SHA-256 value defined in **2.4.1.3. TOE Guidance**. The process for validating the image requires the usage of any software tool capable of calculating the SHA-256 of a given file. For example, the 7-Zip compression/decompression tool includes the capabilities of generating checksum values (hashes). The end user must then, provide the downloaded document (.pdf) to the tool and wait for the generated hash value. Once obtained, the end user will compare the value with the SHA-256 values and determined if they are the same. If the values are identical, then the downloaded image has been properly received and the end user may proceed to perform the installation process. Otherwise, the end user must discard the image and contact Radware technical support via Radware Web Portal <https://support.radware.com> for support in obtaining the correct image.

On the other hand, the end users will have to go to the following section <https://portals.radware.com/Customer/Home/Product-Resources/Products/> in order to get the Alteon Common Criteria Guide and perform the following steps:

a) Scroll down to the Technical Integration Guides section, search for Alteon Common Criteria Guide and download it.



b) Validate the integrity with the SHA-256 value defined in the section **2.4.1.3. TOE Guidance**. The process for validating the image requires the usage of any software tool capable of calculating the SHA-256 of a given file. For example, the 7-Zip compression/decompression

tool includes the capabilities of generating checksum values (hashes). The end user must then, provide the downloaded document (.pdf) to the tool and wait for the generated hash value. Once obtained, the end user will compare the value with the SHA-256 values and determined if they are the same. If the values are identical, then the downloaded image has been properly received and the end user may proceed to perform the installation process. Otherwise, the end user must discard the image and contact Radware technical support via Radware Web Portal <https://support.radware.com> for support in obtaining the correct image.

2.4.1.5 EVALUATED CONFIGURATION

The TOE is configurable to accommodate multiple network topologies with the main constraint being that the back end servers must be accessed through the TOE. The following diagram illustrate the most representative example of a TOE deployment:

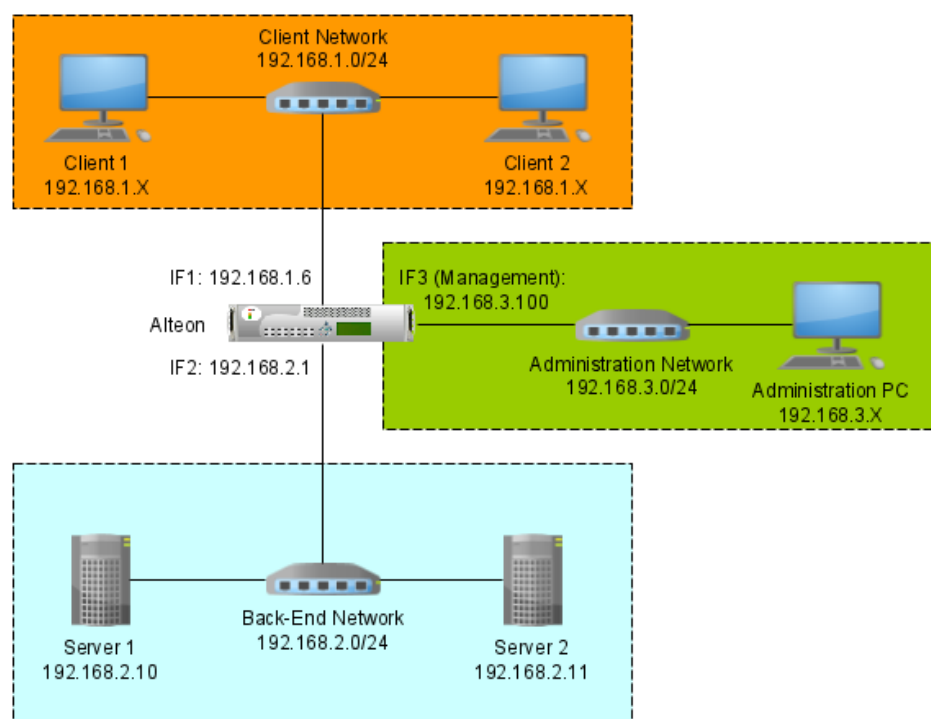


FIGURE 3 - TOE DEPLOYMENT

With the key network segments being:

- Client network for the clients of the virtual load balanced services.
- Back end network for the server that provide the actual services.

- Administration network for separating the Web Management interface (HTTPS) from the data path interface (INGRESS AND EGRESS PORTS).

As illustrated, the TOE is connected all three network segments and acts as the frontend of the virtual services, which are provided by multiple back end servers and whose loads are distributed according to the load balancing rules configured in the TOE.

While the TOE offers support for other complementary external services like RADIUS remote authentication, DefensePro integration. These fall outside of the scope of the evaluation and are not needed in the evaluated configuration. Section **2.4.2 Logical Scope** elaborates on the functionality inside the scope (TSF).

Furthermore, some specific configuration must be followed in order to maintain security in the evaluated configuration (i.e. bypass of the TSF):

- The SSH interface must be disabled.
- The Telnet interface must be disabled.
- The XML API must be disabled.
- The Web Management interface (HTTPS) must use an imported certificate with a RSA key size of 4096 bit.
- The Web Management interface (HTTPS) must be configured to only use TLS1.3.
- Any virtual service created must include an SSL policy which at least:
 - Restrict the cipher suites allowed
 - Use a certificate with a RSA key size of 4096 bit or an EC key size of 256 bit.
- Only local users must be used.
- Management access is restricted to the management network.
- SNMP must be disabled.
- The Extended Log Display must be enabled.
- The automatic session must be configured by the administrator.

For specific details regarding the correct installation and configuration of the TOE, see Alteon Common Criteria Guide.

2.4.2 LOGICAL SCOPE

As described in the Product Introduction and TOE Overview, the TOE is an application delivery controller whose main purpose is to act as a load balancer. From the major features outlined in the Product Introduction only the following ones are part of the logical scope:

- Server Load Balancing for the core function.
- SSL Offloading for providing application layer analysis capabilities.



→ Management Capabilities for managing the configuration and access control.

The following subsections expand more specifically on the TSF in the context of the Common Criteria security requirement families.

2.4.2.1 SECURITY AUDIT

The TOE generates audit records for security-related events across its multiple functional module which are then stored in the local storage. The audit logs are protected from unauthorized modification and deletion.

2.4.2.2 CRYPTOGRAPHIC SUPPORT

The TOE protects the confidentiality and integrity of all of the information passed between the TOE and the authorized administrators, the service clients and the back end servers. The TOE protects these communications by implementing the TLS secure transport protocol.

2.4.2.3 USER DATA PROTECTION

The TOE achieves information flow control applying different policies and rules to the traffic that passes through its data path interfaces (INGRESS AND EGRESS PORTS). Information flow control is used by the TOE to load balance service requests to back end servers in accordance with the rules configured by the administrator.

2.4.2.4 IDENTIFICATION AND AUTHENTICATION

The TOE requires that the users have an associated role, and that they must be identified and authenticated before granting them access to the TOE and its security functions. Users can authenticate through the Web Management interface (HTTPS) using their username and password.


2.4.2.5 SECURITY MANAGEMENT

The TOE provide remote management capabilities via Web Management interface (HTTPS). The security management functionality allows the administrators to configure users, roles and all of the other configuration objects (servers, virtual services, SSL policies, etc.) used in the creation and management of the load balancing rules.

2.4.2.6 PROTECTION OF THE TSF

The TOE provides reliable internal timestamps in order to support the audit functionality.

2.4.2.7 TOE ACCESS



The TOE allows user-initiated and automatic session termination for its Web Management interface (HTTPS). This feature reduces the risk of an attacker using an administrator open session.

2.4.2.8 TRUSTED PATH/CHANNELS

The channels established between the TOE and its remote administrators are protected using TLS1.3 for the Web Management Interface (HTTPS).

Meanwhile, the channels used for communicating between the TOE and the clients/servers is protected using TLS1.2 and TLS1.3, as per mandated in the evaluated configuration.

2.4.2.9 FUNCTIONALITY OUTSIDE OF THE SCOPE

The following TOE functionality falls outside of the scope of the evaluation and will not be evaluated:

- Server health checks
- Application SLA Assurance implementing the high availability and clustering capabilities.
- Web Performance Optimization implementing optimization technologies with FastView.
- Application SLA Monitoring implementing advanced monitoring and application performance metrics.
- Application Firewall implementing an application layer firewall capabilities with AppWall.
- Layered Security Architecture implementing additional security features.
- Review Logs Stored in the TOE

2.4.2.9.1 OPTIONAL SYSLOG

The TOE has the capability to export the audit events to external syslog servers. This functionality is optional and in order to use it the administrator must have a syslog server on the management network. The syslog support is not part of the TSF, and its usage does not impact the internal storage capabilities of the TOE.

The TOE can be configured to use both, the BSD (RFC3164) or the IETF (RFC5424) formats. And additionally, it can be configured to use syslog on top of TLS, thus providing support for the different syslog server configurations.

Recommendations are included in the Alteon Common Criteria Guide.

3. Conformance Claims

3.1 COMMON CRITERIA CONFORMANCE CLAIM

This Security Target is conformant to version 3.1 of Common Criteria for Information Technology Security Evaluation according to:

- Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model; CCMB-2017-04-001, Version 3.1, Revision 5, April 2017
- Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components; CCMB-2017-04-002, Version 3.1, Revision 5, April 2017
- Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Requirements; CCMB-2017-04-003, Version 3.1, Revision 5, April 2017

Being:

- CC Part 2 extended
- CC Part 3 conformant

And claiming conformance with Evaluation Assurance Level 2 (EAL2).

3.2 PROTECTION PROFILE CONFORMANCE CLAIM

The TOE for this ST does not claim conformance with any Protection Profile (PP).

3.3 PACKAGE CLAIM

This Security Target claims conformance to Evaluation Assurance Level 2.

3.4 CONFORMANCE RATIONALE

The TOE for this ST does not claim conformance with any PP, therefore a conformance rationale is not applicable.

4. Security Problem Definition

4.1 TOE ASSETS

The following assets are to be protected by the TOE.

4.1.1 AS.CONFIGURATION

The authenticity and integrity of the TOE configuration.

4.1.2 AS.LOGS

The integrity of the TOE audit logs.

4.1.3 AS.CREDENTIALS

The confidentiality of the TOE user's authentication data (passwords).

4.1.4 AS.DATA

The authentication, confidentiality and integrity of the data going through the TOE.

4.1.5 AS.CORE_FUNCTIONALITY

The availability of the TOE load balancing capabilities.

4.2 THREATS

The following threats are addressed by the TOE. Each threat is described in terms of agents and the actions they can use to compromise the assets described in the previous sections.

4.2.1 T.PASSWORD_CRACKING

Unauthorized users may be able to take advantage of unrestricted authentication attempts to guess the administrative passwords (**AS.CREDENTIAL**) and gain privileged access to the device. Thus, an attacker can misuse the TSF to extract the user authentication data.

4.2.2 T.UNDETECTED_ACTIVITIES

Unauthorized users may attempt to access, change, and/or modify the security functionality of the TOE without Administrator awareness (**AS.LOGS**). This could result in the attacker finding an avenue (e.g., misconfiguration, flaw in the product) to compromise the TOE (**AS.CONFIGURATION**) and the Administrator would have no knowledge that the device has been compromised.

4.2.3 T.WEAK_CRYPTOGRAPHY

An attacker may exploit weak cryptographic algorithms or perform a cryptographic exhaust against the key space. Poorly chosen encryption algorithms, modes, and key sizes will allow attackers to compromise the algorithms, or brute force exhaust the key space and give them unauthorized access allowing them to read, manipulate and/or control the traffic data (**AS.DATA**, **AS.CREDENTIALS**) with minimal effort.

4.2.4 T.WEAK_ENDPOINTS

An attacker may take advantage of secure protocols that use weak methods to authenticate the endpoints – e.g. a shared password that is guessable or transported as plaintext. The consequences are the same as a poorly designed protocol, the attacker could masquerade as the Administrator or another device, and the attacker could insert themselves into the network stream and perform a man-in-the-middle attack. The result is the critical network traffic is exposed (**AS.DATA**, **AS.CREDENTIALS**) and there could be a loss of confidentiality and integrity, and potentially the TOE itself could be compromised.

4.2.5 T.UNBALANCED_LOAD

An attacker may take advantage of an error on the TOE implementation to prevent the application of the load balancing rules configured by the end users. Bypassing or tampering with the TOE load balancing capabilities means that an attacker would compromise of the TOE capabilities (**AS.CORE_FUNCTIONALITY**), causing uncontrolled access to server resources.

4.3 ORGANIZATIONAL POLICIES

The Organizational Security Policies (OSPs) are a set of rules, procedures or guidelines imposed by an organization in the operational environment. Alternatively, the OSPs can also be laid down by legislative or regulatory bodies.

4.3.1 OSP.ROLES

The TOE shall support and implement user management based on user roles.

4.3.2 OSP.LOGS

All management actions must be registered in the audit log.

4.3.3 OSP.ACCOUNTABILITY

All users shall be accountable for their actions within the TOE.

4.3.4 OSP.TRUSTED_ADMINISTRATORS

Only approved and capable individuals shall have administrative access to the TOE.

4.4 ASSUMPTIONS

The following assumptions are assumed to be fulfilled in the operational environment.

4.4.1 A.PHYSICAL_PROTECTION

The TOE is assumed to be physically protected in its operational environment and not subject to physical attacks nor provide physical access to unauthorized users.

4.4.2 A.MANAGEMENT_SEPARATION

The administrative network, by which the TOE administrators connect to the TOE, is assumed to be completely separated from the data path network; only accessible to authorized personnel; and can be considered trustworthy.

4.4.3 A.NO_EVIL

The TOE administrators are assumed to be properly trained, not careless, willfully negligent, or hostile, and will follow all administrative guidance. Furthermore, the supporting environment (Hardware and Virtualization platform) is assumed to be trustworthy and will provide all of the necessary functionality according to the needs of the TOE.

4.4.4 A.LIMITED_FUNCTIONALITY

The TOE is assumed to be used to provide only its core functionality as a load balancer and not provide functionality/services that could be deemed as general purpose computing.

5. Security Objectives

The purpose of the security objectives is to address the security concerns (threats) previously identified and to show which security concerns are addressed by the TOE, and which are addressed by the environment. The following subsections elaborate on the objectives for the two categories of security objectives as per the CC standard:

- Security objectives for the TOE
- Security objectives for the environment.

5.1 SECURITY OBJECTIVES FOR THE TOE

This section identifies and describe the security objectives for the TOE.

5.1.1 O.ACCESS

The TOE must only allow authorized users access to the management capabilities of the TOE and provide the security mechanism to protect the credentials used to provide said access.

5.1.2 O.ADMINISTRATION

The TOE must restrict the functionality available to the users based on their associated role and limit the actions available to all users.

5.1.3 O.AUDIT

The TOE must provide auditing functionality in the form of:

1. Generating audit logs.
2. Storing audit logs.

For all actions performed in the TOE related to the TSF, and be capable of storing the necessary information associated with said actions (user, time, results, etc.).

5.1.4 O.TRUSTED_CHANNELS

The TOE must protect the confidentiality, authenticity and integrity of:

1. Data passed between itself and the authorized administrators.
2. Traffic data passing through the data paths (Ingress and Egress Port).

By means of trusted channels implemented with high security transmission protocols (TLS).

5.1.5 O.TRAFFIC_FLOW

The TOE must ensure that all traffic passing through the data paths (Ingress and Egress Port) have all of the configured load balancing rules properly applied as per the user configuration.

5.2 SECURITY OBJECTIVES FOR THE OPERATIONAL ENVIRONMENT

This section identifies and describes the security objectives for the operational environment.

5.2.1 OE.TRUSTED_ADMINS

The TOE administrators are properly trained and follow all security guidelines to ensure the security of the TOE is maintained. Additionally, the TOE administrators will maintain a completely separated trusted administrative network to access the TOE Web Management interface(HTTPS).

5.2.2 OE.PHYSICAL_SECURITY

The TOE is located in a secure physical location with the appropriate security measure to ensure no physical access is allowed to non-authorized users. Furthermore, the physical supporting hardware or virtualization environment will be equally protected against unauthorized access or manipulation.

5.2.3 OE.NO_GENERAL_PURPOSE

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. The TOE is not configured to provide any non-TSF related service or functionality.

5.3 SECURITY OBJECTIVES RATIONALE

The following table provides a mapping between the threats, organizational policies and assumptions to the security objectives for the TOE and the operational environment.

	T.PASSWORD_CRACKING	T.UNDETECTED_ACTIVITIES	T.WEAK_CRYPTOGRAPHY	T.WEAK_ENDPOINTS	T.UNBALANCED_LOAD	OSP.ROLES	OSP.LOGS	OSP.ACCOUNTABILITY	OSP.TRUSTED_ADMINISTRATORS	A.PHYSICAL_PROTECTION	A.MANAGEMENT_SEPARATION	A.NO_EVIL	A.LIMITED_FUNCTIONALITY
O.ACCESS	X								X				
O.ADMINISTRATION						X			X				
O.AUDIT		X					X	X					
O.TRUSTED_CHANNELS			X	X									
O.TRAFFIC_FLOW					X								
OE.PHYSICAL_SECURITY										X		X	
OE.TRUSTED_ADMINS									X		X	X	
OE.NO_GENERAL_PURPOSE													X

TABLE 6 - SECURITY PROBLEM DEFINITION MAPPING

5.3.1 THREATS

T.PASSWORD_CRACKING: Attacks directed at users accounts and credentials are addressed by the TOE through the security objective **O.ACCESS** which ensures that the TOE implements the necessary security mechanism that prevent password cracking.

T.UNDETECTED_ACTIVITIES: This threat is addressed by keeping a secure audit trail by means of the security objective **O.AUDIT** which register all TSF-related actions being made in the TOE.

T.WEAK_CRYPTOGRAPHY: Attacks intended to break the cryptographic primitives used to protect the data transmitted by the TOE are addressed with the security objective **O.TRUSTED_CHANNELS** which enforces the use of high security algorithms.

T.WEAK_ENDPOINTS: Attacks intended to break the security of the trusted channels by attacking the endpoints are addressed with the security objective **O.TRUSTED_CHANNELS** which enforces a restrictive set high security protocols to be used by the TOE when negotiating with other entities.

T.UNBALANCED_LOAD: This threat is addressed by establishing the necessary mechanism to define and manage all user configurable load balancing rules, and being capable to enforce said rules during nominal operation. This is implemented by means of the security objective **O.TRAFFIC_FLOW**.

5.3.2 ORGANIZATIONAL SECURITY POLICIES

OSP.ROLES: This organizational security policy enforces the usage of role-based user management and it is implemented via the security objective **O.ADMINISTRATION**.

OSP.LOGS: This organizational security policy requires the implementation of an audit management system. The TOE is required to generate, store and allow access to the audit logs generated during operation as dictated by the security objective **O.AUDIT**.

OSP.ACCOUNTABILITY: This organizational security policy requires the association between actions performed in the TOE and the users who performed them. The TOE fulfils this policy by means of the security objective **O.AUDIT** which implements an audit management system which stores all relevant information, including user information, for all TSF-relevant events.

OSP.TRUSTED_ADMINISTRATORS: This organizational security policy requires that all administrative actions are performed only by capable and authorized users. The security objectives **O.ACCESS** and **O.ADMINISTRATION** contribute to enforce this policy by implementing the security mechanism necessary to restrict access to the TOE and it's functionality to the appropriate users.


This is further compounded by the security objective for the operational environment **OE.TRUSTED_ADMINS** which ensures that the TOE administrators will be properly trained and be responsible.

5.3.3 ASSUMPTIONS

A.PHYSICAL_PROTECTION: This assumptions is fully covered by the security objective for the operational environment **OE.PHYSICAL_SECURITY** which ensures that no physical access will be given to unauthorized users.

A.MANAGEMENT_SEPARATION: This assumptions is fully covered by the security objective for the operational environment **OE.TRUESTED_ADMINS** which ensures that the administrators will deploy the TOE such that the Web Management interface (HTTPS) will be only available through a secure management network only available to authorized personnel.

A.NO_EVIL: This assumption is covered by the security objective for the operational environment **OE.TRUSTED_ADMINS** which ensures that the TOE administrators are properly trained and will



follow all administrative guidelines. Furthermore, the objective ***OE.PHYSICAL_SECURITY*** ensures that the supporting hardware environment of the TOE is secure and reliable.

A.LIMITED_FUNCTIONALITY: This assumption is fully covered by the security objective for the operational environment ***OE.NO_GENERAL_PURPOSE*** which ensures that the TOE will not be used for other functions or services that are not related to its core load balancing capabilities.

6. Extended Component Definition

6.1 EXTENDED SECURITY FUNCTIONAL REQUIREMENTS

The Security Functional Requirements included in this section are derived from Part 2 of the Common Criteria for Information Technology Security Evaluation and are intended to be an expansion for covering higher level security protocols.

6.1.1 CLASS FCS: CRYPTOGRAPHIC SUPPORT

The TSF may employ cryptographic functionality to help satisfy several high-level security objectives. These include (but are not limited to): identification and authentication, non-repudiation, trusted path, trusted channel and data separation. This class is used when the TOE implements cryptographic functions, the implementation of which could be in hardware, firmware and/or software.

The FCS: Cryptographic support class is composed of two families: Cryptographic key management (FCS_CKM) and Cryptographic operation (FCS_COP). The Cryptographic key management (FCS_CKM) family addresses the management aspects of cryptographic keys, while the Cryptographic operation (FCS_COP) family is concerned with the operational use of those cryptographic keys.

However, to include higher level protocols new families are being introduced: HTTPS Protocol (FCS_HTS) and TLS Protocol (FCS_TLS). Both families manage the correct implementation of their corresponding protocol (HTTPS & TLS).

6.1.1.1 FCS_HTS: HTTPS PROTOCOL

Family behavior

Components in this family define the requirements for protecting remote management sessions between the TOE and its administrators. This family describes how HTTPS will be implemented.

This family should be included whenever the TSF implements an administrative interface via the HTTPS protocol.

Component levelling

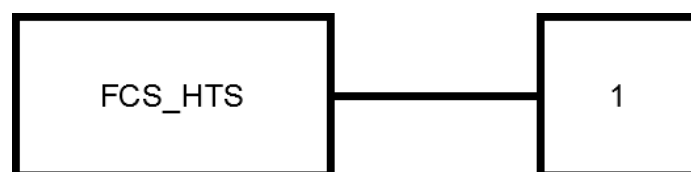


FIGURE 4 - FCS_HTS FAMILY

FCS_HTS.1 HTTPS Protocol for Servers, requires the implementation of the HTTPS protocol by server following the published standards and specify optional peer authentication.

Management: FCS_HTS.1

No management activities are foreseen for this component.

Audit: FCS_HTS.1

There are no auditable events foreseen for this component.

6.1.1.1.1 FCS_HTS.1: HTTPS PROTOCOL FOR SERVERS

Hierarchical to: No other components.

Dependencies: FCS_TLS.1 TLS Protocol for Clients

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

FCS_HTS.1.2 The TSF shall implement HTTPS using TLS.

6.1.1.2 FCS_TLS: TLS PROTOCOL

Family behavior

This family is intended to support the secure implementation of the Transport Layer Security (TLS) by restricting the implementation to use only the high security primitives.

The family should be included whenever the TSF implements trusted channels or trusted path with the TLS protocol.

Component levelling

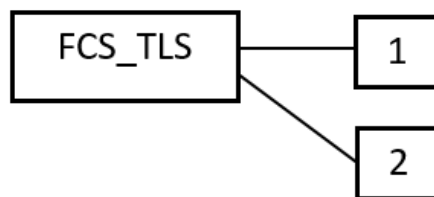


FIGURE 5 - FCS_TLS FAMILY

FCS_TLS.1 TLS Protocol for Clients, requires the implementation of the TLS protocol in order to provide to clients an implementation following the published standards for each selected version.

FCS_TLS.2 TLS Protocol for Servers, requires the implementation of the TLS protocol by servers following the published standards for each selected version.

Management: FCS_TLS.1

No management activities are foreseen for this component.

Audit: FCS_TLS.1

There are no auditable events foreseen for this component.

6.1.1.2.1 FCS_TLS.1: TLS PROTOCOL FOR CLIENTS

Hierarchical to: No other components.

Dependencies: [FTP_ITC.1: Inter-TSF trusted channel, or
FTP_TRP.1: Trusted path].

FCS_TLS.1.1 The TSF shall implement [selection: TLS 1.2 (RFC 5246), TLS 1.3 (RFC 8446)] and reject all other TLS and SSL versions. The TLS implementation will support the following cipher suites: [selection:

- TLS_RSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5246
- TLS_RSA_WITH_AES_256_CBC_SHA256 as defined in RFC 5246
- TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5246
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 as defined in RFC 5246
- TLS_RSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5288
- TLS_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5288
- TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5288
- TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5288
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5289
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 as defined in RFC 5289
- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5289
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5289
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5289
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 as defined in RFC 5289
- TLS_AES_128_GCM_SHA256 as defined in RFC 8446
- TLS_AES_256_GCM_SHA384 as defined in RFC 8446
- TLS_AES_128_CCM_SHA256 as defined in RFC 8446
- TLS_AES_128_CCM_8_SHA256 as defined in RFC 8446
- TLS_CHACHA20_POLY1305_SHA256 as defined in RFC 8446

].

FCS_TLS.1.2 The TSF shall deny connections from clients requesting SSL 2.0, SSL 3.0, TLS 1.0, TLS 1.1 and [selection: TLS 1.2, TLS 1.3, none].

FCS_TLS.1.3 The TSF shall [selection:

- perform RSA key establishment with key size [selection: 2048 bits, 3072 bits, 4096 bits];
- generate EC Diffie-Hellman parameters over curves [assignment: *list of supported curves*] and no other curves;
- generate Diffie-Hellman parameters of size [selection: 2048 bits, 3072 bits]

].

6.1.1.2.2 FCS_TLS.2: TLS PROTOCOL FOR SERVERS

Hierarchical to: No other components.

Dependencies: [FTP_ITC.1: Inter-TSF trusted channel].

FCS_TLS.2.1 The TSF shall implement [selection: TLS 1.2 (RFC 5246), TLS 1.3 (RFC 8446)] and reject all other TLS and SSL versions. The TLS implementation will support the following cipher suites: [selection:

- TLS_RSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5246
- TLS_RSA_WITH_AES_256_CBC_SHA256 as defined in RFC 5246
- TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5246
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 as defined in RFC 5246
- TLS_RSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5288
- TLS_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5288
- TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5288
- TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5288
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5289
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 as defined in RFC 5289
- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5289
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5289
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5289
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 as defined in RFC 5289
- TLS_AES_128_GCM_SHA256 as defined in RFC 8446
- TLS_AES_256_GCM_SHA384 as defined in RFC 8446

- TLS_AES_128_CCM_SHA256 as defined in RFC 8446
- TLS_AES_128_CCM_8_SHA256 as defined in RFC 8446
- TLS_CHACHA20_POLY1305_SHA256 as defined in RFC 8446

].

FCS_TLS.2.2 The TSF shall deny connections of servers offering SSL 2.0, SSL 3.0, TLS 1.0, TLS 1.1 and [selection: TLS 1.2, TLS 1.3, none].

FCS_TLS.2.3 The TSF shall [selection:

- perform RSA key establishment with key size [selection: 2048 bits, 3072 bits, 4096 bits];
- generate EC Diffie-Hellman parameters over curves [assignment: *list of supported curves*] and no other curves;
- generate Diffie-Hellman parameters of size [selection: 2048 bits, 3072 bits]

].

7. Security Requirements

7.1 CONVENTIONS

In accordance with Part 1 of the Common Criteria standard, there are four types of operation applicable for SFRs and SARs. For each type of operation, the following typographical distinctions will apply:

1. Iteration: iterations will have a text extension (with format “/” + “label”) added at the end for name. For example, FCS_COP.1/AES and FCS_COP.1/SHA.
2. Assignment: assignments are surrounded by brackets and the inner text will be in italics. For example, [*assigned item*].
3. Selection: selections are surrounded by brackets. For example, [selected item].
4. Refinement: refinements are marked depending on their type. For added information the text will be in **bold**; meanwhile, any removed text will be ~~strikeout~~. For example, users will provide ~~original item~~ **new item** when...

7.2 SECURITY FUNCTIONAL REQUIREMENTS

The following Security Functional Requirements have been selected from Part 2 of the common criteria standard, together with the extended requirements as defined in section 6.1:

Class	Identifier	Name
Security Audit (FAU)	FAU_GEN.1	Audit data generation
	FAU_GEN.2	User identity association
	FAU_STG.1	Protected audit trail storage
	FAU_STG.4	Prevention of audit data loss
Cryptographic Support (FCS)	FCS_CKM.2	Cryptographic key distribution
	FCS_CKM.4	Cryptographic key destruction
	FCS_HTS.1	HTTPS Protocol for Servers
	FCS_TLS.1/WBM	TLS Protocol for Clients
	FCS_TLS.1/DATA	TLS Protocol for Clients
	FCS_TLS.2	TLS Protocol for Servers
User Data Protection (FDP)	FDP_IFC.1	Subset information flow control
	FDP_IFF.1	Simple security attributes
Identification and Authentication (FIA)	FIA_AFL.1	Authentication failure handling
	FIA_UAU.2	User authentication before any action
	FIA_UID.2	Timing of identification

Class	Identifier	Name
Security Management (FMT)	FMT_MSA.1	Management of security attributes
	FMT_MSA.3	Static attribute initialisation
	FMT_SMF.1	Specification of management functions
	FMT_SMR.2	Restrictions on security roles
Protection of the TSF (FPT)	FPT_STM.1	Reliable time stamps
TOE Access (FTA)	FTA_SSL.3	TSF-initiated termination
	FTA_SSL.4	User-initiated termination
Trusted Path/Channels (FTP)	FTP_ITC.1	Inter-TSF trusted channel
	FTP_TRP.1	Trusted path

TABLE 7 - SECURITY FUNCTIONAL REQUIREMENT SUMMARY

7.2.1 SECURITY AUDIT (FAU)

7.2.1.1 FAU_GEN.1: AUDIT DATA GENERATION

Hierarchical to: No other components.

Dependencies: FPT_STM.1 Reliable time stamps

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

- a) Start-up and shutdown of the audit functions;
- b) All auditable events for the [not specified] level of audit; and
- c) [*The following events:*
 - *User login*
 - *User logout*
 - *Applying changes to TOE configuration*
 - *Saving changes of TOE configuration to disk*
 - *Errors when applying an invalid configuration.*
 - *Changes to the user's passwords*

].

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

- a) Date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event; and

- b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [*none*].

7.2.1.2 FAU_GEN.2: USER IDENTITY ASSOCIATION

- Hierarchical to: No other components.
Dependencies: FAU_GEN.1 Audit data generation
FIA_UID.1 Timing of identification

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.

7.2.1.3 FAU_STG.1: PROTECTED AUDIT TRAIL STORAGE

- Hierarchical to: No other components.
Dependencies: FAU_GEN.1 Audit data generation

FAU_STG.1.1 The TSF shall protect the stored audit records in the audit trail from unauthorised deletion.

FAU_STG.1.2 The TSF shall be able to [prevent] unauthorised modifications to the stored audit records in the audit trail.

7.2.1.4 FAU_STG.4: PREVENTION OF AUDIT DATA LOSS

- Hierarchical to: FAU_STG.3 Action in case of possible audit data loss
Dependencies: FAU_STG.1 Protected audit trail storage

FAU_STG.4.1 The TSF shall [overwrite the oldest stored audit records] and [*no other action*] if the audit trail is full.

7.2.2 CRYPTOGRAPHIC SUPPORT (FCS)

7.2.2.1 FCS_CKM.2: CRYPTOGRAPHIC KEY DISTRIBUTION

- Hierarchical to: No other components.
Dependencies: FCS_CKM.1 Cryptographic key generation
FCS_CKM.4 Cryptographic key destruction

FCS_CKM.2.1 The TSF shall distribute cryptographic keys in accordance with a specified cryptographic key distribution method [*key distribution via transport layer protocol*] that meets the following: [*RFC8446 and RFC5246*].

Application note: They key distribution is implemented as part of the secure transport protocol TLS, in accordance with the respective standard.

7.2.2.2 FCS_CKM.4: CRYPTOGRAPHIC KEY DESTRUCTION

Hierarchical to: No other components.

Dependencies: FCS_CKM.1 Cryptographic key generation

FCS_CKM.4.1 The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method [*removing stored instances*] that meets the following: [*no standards*].

7.2.2.3 FCS_HTTPS.1: HTTPS PROTOCOL FOR SERVERS

Hierarchical to: No other components.

Dependencies: FCS_TLS.1 TLS Protocol for Clients

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

FCS_HTTPS.1.2 The TSF shall implement HTTPS using TLS.

7.2.2.4 FCS_TLS.1/WBM: TLS PROTOCOL FOR CLIENTS

Hierarchical to: No other components.

Dependencies: FTP_TRP.1: Trusted path

FCS_TLS.1.1 The TSF shall implement [TLS 1.3 (RFC 8446)] and reject all other TLS and SSL versions. The TLS implementation will support the following ciphersuites: [

- TLS_AES_128_GCM_SHA256 as defined in RFC 8446
- TLS_AES_256_GCM_SHA384 as defined in RFC 8446
- TLS_CHACHA20_POLY1305_SHA256 as defined in RFC 8446

].

Application note: In [SOGIS-ACM], algorithms such as CHACHA20 and POLY1305 have not been defined as either recommended or legacy. However, following the recommendation in section 9.1

Mandatory-to-Implement Cipher Suites of [RFC8446] the cipher suite TLS_CHACHA20_POLY1305_SHA256 has been implemented as part of the TLS 1.3 support.

FCS_TLS.1.2 The TSF shall deny connections from clients requesting SSL 2.0, SSL 3.0, TLS 1.0, TLS 1.1 and [TLS 1.2].

FCS_TLS.1.3 The TSF shall [generate EC Diffie-Hellman parameters over curves [*secp256r1, secp384r1, secp521r1, curve25519, curve448*] and no other curves; generate Diffie-Hellman parameters of size [2048 bits]].

7.2.2.5 FCS_TLS.1/DATA: TLS PROTOCOL FOR CLIENTS

Hierarchical to: No other components.

Dependencies: FTP_ITC.1: Inter-TSF trusted channel

FCS_TLS.1.1 The TSF shall implement [TLS 1.2 (RFC 5246) and TLS 1.3 (RFC 8446)] and reject all other TLS and SSL versions. The TLS implementation will support the following ciphersuites: [

- TLS_RSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5246
 - TLS_RSA_WITH_AES_256_CBC_SHA256 as defined in RFC 5246
 - TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5246
 - TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 as defined in RFC 5246
 - TLS_RSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5288
 - TLS_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5288
 - TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5288
 - TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5288
 - TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5289
 - TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 as defined in RFC 5289
 - TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5289
 - TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289
 - TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5289
 - TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289
 - TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5289
 - TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 as defined in RFC 5289
 - TLS_AES_128_GCM_SHA256 as defined in RFC 8446
 - TLS_AES_256_GCM_SHA384 as defined in RFC 8446
 - TLS_CHACHA20_POLY1305_SHA256 as defined in RFC 8446
-].

Application note: In [SOGIS-ACM], several of the selected ciphersuites are designated as “Legacy”, but for compatibility purposes these ciphersuites are supported in the TOE.

Furthermore, algorithms such as CHACHA20 and POLY1305 have not been defined as either recommended or legacy. However, following the recommendation in section **9.1 Mandatory-to-Implement Cipher Suites** of [RFC8446] the cipher suite TLS_CHACHA20_POLY1305_SHA256 has been implemented as part of the TLS 1.3 support.

FCS_TLS.1.2 The TSF shall deny connections from clients requesting SSL 2.0, SSL 3.0, TLS 1.0, TLS 1.1 and [none].

FCS_TLS.1.3 The TSF shall [generate EC Diffie-Hellman parameters over curves [*secp256r1, secp384r1, secp521r1, curve25519, curve448*] and no other curves; generate Diffie-Hellman parameters of size [2048 bits]].

7.2.2.6 FCS_TLS.2: TLS PROTOCOL FOR SERVERS

Hierarchical to: No other components.

Dependencies: FTP_ITC.1: Inter-TSF trusted channel

FCS_TLS.2.1 The TSF shall implement [TLS 1.2 (RFC 5246) and TLS 1.3 (RFC 8446)] and reject all other TLS and SSL versions. The TLS implementation will support the following ciphersuites: [

- TLS_RSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5246
- TLS_RSA_WITH_AES_256_CBC_SHA256 as defined in RFC 5246
- TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5246
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 as defined in RFC 5246
- TLS_RSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5288
- TLS_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5288
- TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5288
- TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5288
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5289
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 as defined in RFC 5289
- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5289
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5289
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289

- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5289
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 as defined in RFC 5289
- TLS_AES_128_GCM_SHA256 as defined in RFC 8446
- TLS_AES_256_GCM_SHA384 as defined in RFC 8446
- TLS_CHACHA20_POLY1305_SHA256 as defined in RFC 8446

].

Application note: In [SOGIS-ACM], several of the selected ciphersuites are designated as “*Legacy*”, but for compatibility purposes these ciphersuites are supported in the TOE.

Furthermore, algorithms such as CHACHA20 and POLY1305 have not been defined as either recommended or legacy. However, following the recommendation in section **9.1 Mandatory-to-Implement Cipher Suites** of [RFC8446] the cipher suite TLS_CHACHA20_POLY1305_SHA256 has been implemented as part of the TLS 1.3 support.

FCS_TLS.2.2 The TSF shall deny connections of servers offering SSL 2.0, SSL 3.0, TLS 1.0, TLS 1.1 and [none].

FCS_TLS.2.3 The TSF shall [generate EC Diffie-Hellman parameters over curves [*secp256r1, secp384r1, secp521r1, curve25519, curve448*] and no other curves; generate Diffie-Hellman parameters of size [2048 bits]].

7.2.3 USER DATA PROTECTION (FDP)

7.2.3.1 FDP_IFC.1: SUBSET INFORMATION FLOW CONTROL

Hierarchical to: No other components.

Dependencies: FDP_IFF.1 Simple security attributes

FDP_IFC.1.1 The TSF shall enforce the [*Load Balancing Policy*] on [

- *Subjects: Real servers*
- *Information: Service requests*
- *Operations: Access*

].

7.2.3.2 FDP_IFF.1: SIMPLE SECURITY ATTRIBUTES

Hierarchical to: No other components.

Dependencies: FDP_IFC.1 Subset information flow control

FMT_MSA.3 Static attribute initialization

- FDP_IFF.1.1** The TSF shall enforce the [*Load Balancing Policy*] based on the following types of subject and information security attributes: [
- *Subjects:*
 - *Real servers:*
 - *Server groups*
 - *Authentication policy*
 - *Number of connections*
 - *Response time*
 - *Bandwidth available*
 - *Information:*
 - *Service requests:*
 - *Source IP address*
 - *Source port*
 - *Virtual IP address target*
 - *Virtual port target*
-].
- FDP_IFF.1.2** The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: [*a given request for service is only forwarded to a single real server based on the configuration attributes of the load balancing rules of the target virtual service*].
- FDP_IFF.1.3** The TSF shall enforce the [*no additional rules*].
- FDP_IFF.1.4** The TSF shall explicitly authorise an information flow based on the following rules: [*none*].
- FDP_IFF.1.5** The TSF shall explicitly deny an information flow based on the following rules: [*none*].

Application note: In FDP_IFF.1.2, “*configuration attributes of the load balancing rules*” refer to a combination of the attributes listed in FDP_IFF.1.1 since depending on the algorithm selected some may be used while others may not.

7.2.4 IDENTIFICATION AND AUTHENTICATION (FIA)

7.2.4.1 FIA_AFL.1: AUTHENTICATION FAILURE HANDLING

Hierarchical to: No other components.

Dependencies: FIA_UAU.1 Timing of authentication

FIA_AFL.1.1 The TSF shall detect when [an administrator configurable positive integer within [3 and 100]] unsuccessful authentication attempts occur **between an administrator configurable range of time, between 1 and 60 minutes**, related to [user login].

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been [met], the TSF shall [lock the user account for a configurable amount of time between 0 and 3600 minutes].

7.2.4.2 FIA_UAU.2: USER AUTHENTICATION BEFORE ANY ACTION

Hierarchical to: FIA_UAU.1 Timing of authentication

Dependencies: FIA_UID.1 Timing of identification

FIA_UAU.2.1 The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

7.2.4.3 FIA_UID.2: TIMING OF IDENTIFICATION

Hierarchical to: FIA_UID.1 Timing of identification

Dependencies: No dependencies.

FIA_UID.2.1 The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

7.2.5 SECURITY MANAGEMENT (FMT)

7.2.5.1 FMT_MSA.1: MANAGEMENT OF SECURITY ATTRIBUTES

Hierarchical to: No other components.

Dependencies: FDP_IFC.1 Subset information flow control

FMT_SMR.1 Security roles

FMT_SMF.1 Specification of management functions

FMT_MSA.1.1 The TSF shall enforce the [*Load Balancing Policy*] to restrict the ability to [query, modify] the security attributes [*of real servers*]:

- *Server groups*
- *Authentication policy*
- *Number of connections*
- *Bandwidth available*

] to [

- *Administrators*
- *L4 Administrators*
- *SLB Administrators*

].

7.2.5.2 FMT_MSA.3: STATIC ATTRIBUTE INITIALIZATION

Hierarchical to: No other components.

Dependencies: FMT_MSA.1 Management of security attributes
FMT_SMR.1 Security roles

FMT_MSA.3.1 The TSF shall enforce the [*Load Balancing Policy*] to provide [permissive] default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2 The TSF shall allow the [*Administrator, L4 administrator and SLB administrator*] to specify alternative initial values to override the default values when an object or information is created.

Application note: The three allowed roles are a subset of the TOE roles defined in FMT_SMR.2 with the same name.

7.2.5.3 FMT_SMF.1: SPECIFICATION OF MANAGEMENT FUNCTIONS

Hierarchical to: No other components.

Dependencies: No dependencies.

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

[

- *Create TOE users*
- *Modify TOE users*

- *Delete TOE users*
- *Create back end servers*
- *Modify back end servers*
- *Delete back end servers*
- *Create virtual servers*
- *Modify virtual servers*
- *Delete virtual servers*
- *Import TOE certificates*
- *Delete TOE certificates*

].

7.2.5.4 FMT_SMR.2: RESTRICTIONS ON SECURITY ROLES

Hierarchical to: FMT_SMR.1 Security roles

Dependencies: FIA_UID.1 Timing of identification

FMT_SMR.2.1 The TSF shall maintain the roles: [*User, Operator, Administrator, Certificate Administrator, SLB Viewer, SLB Operator, SLB Administrator, L4 Administrator and L4 Operator*].

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 [

- *users may only have one role*

] are satisfied.

Application Note: The TOE shows some non-working roles (L3 administrator and L3 operator) in their Web Management interfaces (HTTPS), but these roles are not implemented and just remain as part an UI artifact to be fixed in later versions.

7.2.6 PROTECTION OF THE TSF (FPT)

7.2.6.1 FPT_STM.1: RELIABLE TIME STAMPS

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_STM.1.1 The TSF shall be able to provide reliable time stamps.

7.2.7 TOE ACCESS (FTA)

7.2.7.1 FTA_SSL.3: TSF-INITIATED TERMINATION

Hierarchical to: No other components.

Dependencies: No dependencies.

FTA_SSL.3.1 The TSF shall terminate an interactive session after an *[administrator configurable time period between 1 and 10080 minutes]*.

7.2.7.2 FTA_SSL.4: USER-INITIATED TERMINATION

Hierarchical to: No other components.

Dependencies: No dependencies.

FTA_SSL.4.1 The TSF shall allow user-initiated termination of the user's own interactive session.

7.2.8 TRUSTED PATH (FTP)

7.2.8.1 FTP_ITC.1: INTER-TSF TRUSTED CHANNEL

Hierarchical to: No other components.

Dependencies: No dependencies.

FTP_ITC.1.1 The TSF shall provide a communication channel between itself and another trusted IT product that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.

FTP_ITC.1.2 The TSF shall permit [the TSF, another trusted IT product] to initiate communication via the trusted channel.

FTP_ITC.1.3 The TSF shall initiate communication via the trusted channel for *[redirecting request to the backend servers during load balancing, receiving the request from another trusted IT product during load balancing]*.

7.2.8.2 FTP_TRP.1: TRUSTED PATH

Hierarchical to: No other components.

Dependencies: No dependencies.

- FTP_TRP.1.1** The TSF shall provide a communication path between itself and [remote] users that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from [modification and disclosure].
- FTP_TRP.1.2** The TSF shall permit [remote users] to initiate communication via the trusted path.
- FTP_TRP.1.3** The TSF shall require the use of the trusted path for [initial user authentication and *[all administrative actions]*].

7.3 ASSURANCE SECURITY REQUIREMENTS

The TOE assurance requirements for this ST consist of the requirements corresponding to the EAL2 level of assurance, as defined in the CC Part 3.

The Security Assurance Requirements (SARs) are summarized in the following table:

Assurance Class	SAR ID	SAR Name
Class ADV: Development	ADV_ARC.1	Security architecture description
	ADV_FSP.2	Security-enforcing functional specification
	ADV_TDS.1	Basic design
Class AGD: Guidance Documents	AGD_OPE.1	Operational user guidance
	AGD_PRE.1	Preparative procedures
Class ALC: Life-cycle Support	ALC_CMC.2	Use of a CM system
	ALC_CMS.2	Parts of the TOE CM coverage
	ALC_DEL.1	Delivery procedures
Class ASE: Security Target Evaluation	ASE_CCL.1	Conformance claims
	ASE_ECD.1	Extended components definition
	ASE_INT.1	ST introduction
	ASE_OBJ.2	Security objectives
	ASE_REQ.2	Derived security requirements
	ASE_SPD.1	Security Problem Definition
Class ATE: Tests	ATE_COV.1	Evidence of coverage
	ATE_FUN.1	Functional testing
	ATE_IND.2	Independent testing - sample
Class AVA: Vulnerability Assessment	AVA_VAN.2	Vulnerability analysis

TABLE 8 - SECURITY ASSRUANCE REQUIREMENT SUMMARY

7.4 RATIONALE FOR THE SECURITY REQUIREMENTS

7.4.1 RATIONALE FOR THE SECURITY FUNCTIONAL REQUIREMENTS

The following table provides a mapping between the SFRs and the Security Objectives.

	O.ACCESS	O.ADMINISTRATION	O.AUDIT	O.TRUSTED_CHANNELS	O.TRAFFIC_FLOW
FAU_GEN.1			X		
FAU_GEN.2			X		
FAU_STG.1			X		
FAU_STG.4			X		
FCS_CKM.2				X	
FCS_CKM.4				X	
FCS_HTS.1				X	
FCS_TLS.1/WBM				X	
FCS_TLS.1/DATA				X	
FCS_TLS.2				X	
FDP_IFC.1					X
FDP_IFF.1					X
FIA_AFL.1	X				
FIA_UAU.2	X	X			
FIA_UID.2	X	X			
FMT_MSA.1					X
FMT_MSA.3					X

	O.ACCESS	O.ADMINISTRATION	O.AUDIT	O.TRUSTED_CHANNELS	O.TRAFFIC_FLOW
FMT_SMF.1		X			X
FMT_SMR.2		X			
FPT_STM.1			X		
FTA_SSL.3	X				
FTA_SSL.4	X				
FTP_ITC.1				X	X
FTP_TRP.1				X	X

TABLE 9 - SECURITY REQUIREMENT RATIONALE MAPPING

The following rationale traces each SFR back to the Security Objectives for the TOE:

Objective: O.ACCESS	The TOE must only allow authorized users access to the management capabilities of the TOE and provide the security mechanism to protect the credentials used to provide said access.
Security Functional Requirements	FIA_AFL.1, FIA_UAU.2, FIA_UID.2, FTA_SSL.3 and FTA_SSL.4
Rationale	<p>FIA_AFL.1 supports the objective by locking a user account after a specified number of unsuccessful authentication attempts, thereby protecting the TOE against a brute force attack or password guessing.</p> <p>FIA_UAU.2 and FIA_UID.2 ensure that users are identified and authenticated prior to being granted access to the management capabilities of the TOE.</p> <p>FTA_SSL.3 and FTA_SSL.4 support the objective by ensuring that open sessions can be closed manually or automatically to reduce the risk of an attacker using an open session.</p>

TABLE 10 - RATIONALE FOR O.ACCESS

Objective: O.ADMINISTRATION	The TOE must restrict the functionality available to the users based on their associated role and limit the actions available to all users.
Security Requirements Functional	FIA_UAU.2, FIA_UID.2, FMT_SMF.1 and FMT_SMR.2
Rationale	<p>FMT_SMF.1 supports this objective by defining the list of management functions that can be performed in the TOE by the authorized administrators. FMT_SMR.2 covers this objective by defining the roles which are used to provide access to the TOE security functionality in the different parts of the TOE.</p> <p>FIA_UAU.2 and FIA_UID.2 ensure that users are identified and authenticated prior to being granted access to the actions available to each user of the TOE.</p>

TABLE 11 - RATIONALE FOR O.ADMINISTRATION

Objective: O.AUDIT	<p>The TOE must provide auditing functionality in the form of:</p> <ol style="list-style-type: none"> 1. Generating audit logs. 2. Storing audit logs. <p>For all actions performed in the TOE related to the TSF, and be capable of storing the necessary information associated with said actions (user, time, results, etc.).</p>
Security Requirements Functional	FAU_GEN.1, FAU_GEN.2, FAU_STG.1, FAU_STG.4 and FPT_STM.1
Rationale	<p>FAU_GEN.1 and FAU_GEN.2 meet this objective by ensuring that the TOE generates audit records for the specified set of auditable events and that the audit records associate a user identity with the auditable event.</p> <p>FAU_STG.1 supports this objective by ensuring that the audit trail is protected against deletion and modification.</p> <p>FAU_STG.4 supports this objective specifying how audit data is treated when the audit trail is full.</p> <p>FPT_STM.1 supports this objective by ensuring that the TOE is able to provide the timestamps used in the audit trail.</p>

TABLE 12 - RATIONALE FOR O.AUDIT

Objective:	The TOE must protect the confidentiality, authenticity and integrity of:
-------------------	--

O.TRUSTED_CHANNELS	<ol style="list-style-type: none"> 1. Data passed between itself and the authorized administrators. 2. Traffic data passing through the data paths (Ingress and Egress Port). <p>By means of trusted channels implemented with high security transmission protocols (TLS).</p>
Security Functional Requirements	FCS_CKM.2, FCS_CKM.4, FCS_HTS.1, FCS_TLS.1/WBM, FCS_TLS.1/DATA, FCS_TLS.2, FTP_ITC.1 and FTP_TRP.1
Rationale	<p>FCS_CKM.2 and FCS_CKM.4 support the objective by providing the supporting functionality (certificate management) required to create the trusted channels.</p> <p>FCS_HTS.1 covers this objective defining how the TOE implements the HTTPS protocol used to protect the data sent between the TOE and the authorized administrators.</p> <p>FCS_TLS.1/WBM covers this objective specifying the characteristics of the TLS implementation used by the TOE to create trusted path and protect data passed between the TOE and the authorized administrators.</p> <p>FCS_TLS.1/DATA, similarly, implements a trusted channel between the TOE and the clients endpoints.</p> <p>FCS_TLS.2, similarly, implements a trusted channel between the TOE and the servers endpoints.</p> <p>FTP_ITC.1 and FTP_TRP.1 support the objective by specifying the use of that cryptography between the TOE and the remote administrators, and between the other clients of the TOE.</p>

TABLE 13 - RATIONALE FOR O.TRUSTED_CHANNELS

Objective: O.TRAFFIC_FLOW	The TOE must ensure that all traffic passing through the data paths (Ingress and Egress Port) have all of the configured load balancing rules properly applied as per the user configuration.
Security Functional Requirements	FDP_IFC.1, FDP_IFF.1, FMT_MSA.1, FMT_MSA.3, FMT_SMF.1, FTP_ITC.1 and FTP_TRP.1
Rationale	<p>FDP_IFC.1 and FDP_IFF.1 cover this objective specifying the subjects, operations and security attributes that can be applied and used by the TOE to perform the flow control functionality used to allow access to back end servers via virtual services.</p> <p>FMT_MSA.1 supports this objective by specifying the user roles and</p>



	<p>operations that can be performed over the security attributes used to manage the flow control policies.</p> <p>FMT_MSA.3 supports this objective by specifying the characteristics of the security attributes initialization and the user roles that can specify alternative initial values for such attributes.</p> <p>FMT_SMF.1 defines the management functions necessary for configuring the network traffic rules that are applied as the flow control policies.</p> <p>FTP_ITC.1 and FTP_TRP.1 support this objective by specifying the trusted channels used as basis for the load balancing capabilities.</p>
--	--

TABLE 14 - RATIONALE FOR O.TRAFFIC_FLOW

7.4.1.1 SECURITY FUNCTIONAL REQUIREMENTS DEPENDENCY RATIONALE

The following table provides the dependency rationale for the Security Functional Requirements.

SFR	Dependency	Dependency Rationale
FAU_GEN.1	FPT_STM.1	Included in SFRs
FAU_GEN.2	FAU_GEN.1 FIA_UID.1	FAU_GEN.1 is included in SFRs Hierarchical component FIA_UID.2 has been included in SFRs
FAU_STG.1	FAU_GEN.1	Included in SFRs
FAU_STG.4	FAU_STG.1	Included in SFRs
FCS_CKM.2	[FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2] FCS_CKM.4	FCS_CKM.4 is included in SFRs FCS_CKM.1 is not included as SFR because the TOE should not be used to generate secure certificates, but rather import those generated by a trusted security authority.
FCS_CKM.4	[FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2]	FCS_CKM.1 is not included as SFR because the TOE should not be used to generate secure certificates, but rather import those generated by a trusted security authority.
FCS_HTS.1	FCS_TLS.1	FCS_TLS.1/WBM is included in SFRs
FCS_TLS.1/WBM	[FTP_ITC.1 or FTP_TRP.1]	FTP_TRP.1 is included in SFRs
FCS_TLS.1/DATA	[FTP_ITC.1 or FTP_TRP.1]	FTP_ITC.1 is included in SFRs
FCS_TLS.2	[FTP_ITC.1]	Included in SFRs
FDP_IFC.1	FDP_IFF.1	Included in SFRs

SFR	Dependency	Dependency Rationale
FDP_IFF.1	FDP_IFC.1 FMT_MSA.3	Both included in SFRs
FIA_AFL.1	FIA_UAU.1	Hierarchical component FIA_UAU.2 has been included in SFRs
FIA_UAU.2	FIA_UID.1	Hierarchical component FIA_UID.2 has been included in SFRs
FIA_UID.2	None	N/A
FMT_MSA.1	[FDP_ACC.1 or FDP_IFC.1] FMT_SMR.1 FMT_SMF.1	FDP_IFC.1, and FMT_SMF.1 have been included in SFRs Hierarchical component FMT_SMR.2 has been included in SFRs
FMT_MSA.3	FMT_MSA.1 FMT_SMR.1	FMT_MSA.1 is included in SFRs Hierarchical component FMT_SMR.2 has been included in SFRs
FMT_SMF.1	None	N/A
FMT_SMR.2	FIA_UID.1	Hierarchical component FIA_UID.2 has been included in SFRs
FPT_STM.1	None	N/A
FTA_SSL.3	None	N/A
FTA_SSL.4	None	N/A
FTP_ITC.1	None	N/A
FTP_TRP.1	None	N/A

TABLE 15 - SFR DEPENDENCIES

7.4.2 RATIONALE FOR THE SECURITY ASSURANCE REQUIREMENTS

The TOE assurance requirements for this ST consist of the requirements corresponding to the EAL 2 level of assurance, as defined in the CC Part 3. The EAL 2 package was selected to fulfil the required market level for this kind of products.

Since all the SARs included in this Security Target have been taken from a self-sufficient assurance package (EAL 2), there are no dependencies missing for the selected security assurance requirements.

8. TOE Summary Specification

8.1 DESCRIPTION ON HOW TOE MEETS EACH SFR

8.1.1 SECURITY AUDIT

The TOE provides comprehensive audit management capabilities. The TOE generates audit logs of the module-specific events across all of its functional modules identifying the user that cause it and then store them in the internal storage. The TOE by default stores the audit logs in three rotating files, each holding up to 1.5MB of space, on the internal storage. When the storage files are full the TOE replaces the oldest ones with the newer ones, thus overwriting older records.

TOE Security Functional Requirements covered: FAU_GEN.1, FAU_GEN.2, FAU_STG.1, FAU_STG.4.

8.1.2 CRYPTOGRAPHIC SUPPORT

The TOE implements secure transport channels in order to communicate with the administrators (1), the service clients (2) and the back end servers (3). These secure transport channels are implemented via the HTTPS/TLS protocols and are employed as follows:

- For the Web Management interfaces (HTTPS) the TOE allows web access via HTTPS/TLS. [1]
- For the data path interfaces (INGRESS AND EGRESS PORT) the TOE allows custom configuration of the TLS policies to accommodate restrictive and secure parameters during load balancing. [2, 3]

As part of the core functionality (load balancing) the TOE provides support to manage (import and delete) cryptographic keys associated to certificates for virtual services (TLS certificates) and the Web Management Interface (HTTPS). Since these keys are primarily used to authenticate the TOE to external entities, the generation of such keys is delegated to a trustworthy certificate or registration authority. Therefore, the certificates and their associated keys **must** be imported.

TOE Security Functional Requirements covered: FCS_CKM.2, FCS_CKM.4, FCS_HTS.1, FCS_TLS.1/WBM, FCS_TLS.1/DATA, FCS_TLS.2.

8.1.3 USER DATA PROTECTION

The TOE core functionality is providing load balancing capabilities and it implements it by allowing the creation of virtual services mapped to back end servers following a load balancing configuration. The TOE discards any requests that does not match any existing virtual service and redirect the request based on the load balancing rules defined by the administrators.

TOE Security Functional Requirements covered: FDP_IFC.1, FDP_IFF.1.

8.1.4 IDENTIFICATION AND AUTHENTICATION

The TOE restricts all management functionality to authorized users and will not provide any functionality before login. Based on the associated role to the user, the TOE will provide segmented access to its functionality ranging from a subset of functions or to restrict the ability to modify parameters.

The TOE supports the administration through the Web Management Interface (HTTPS) which must be configured in the evaluated configuration in order to provide high security to its users.

In the evaluated configuration, if the users fail authentication repeatedly within the lockout reset duration, then they are locked for a configurable period of time or until the administrator unlocks the account. In order to ensure that TOE is in the evaluated configuration, the following configuration must be applied:

- The number of failed attempts before lockout must be set in 5.
- The lockout time after perform the maximum fail attempts must be set in 1.
- The timeframe in which the failure threshold must be met for the lockout to trigger must be set in 1.

TOE Security Functional Requirements covered: FIA_AFL.1, FIA_UAU.2, FIA_UID.2.

8.1.5 SECURITY MANAGEMENT

Each user has an associated user role which is used to limit the access to certain parts of the TOE functionality. The following list describes the available roles and their associated functionality:

- User: This role does not possess any management capabilities by default and only has access to status and statistics information of the TOE. Only if it has back end servers associated to the user by an administrator, it will be capable of changing their operational status.
- Operator: This role monitors and manage the back end servers (enabling or disabling them) and the server groups during operation.
- Administrator: This role has the highest level administration privileges with access and control of all of the TOE functionality.
- Certificate Administrator: This role has access to very reduced set of functionality related to the management of the TOE certificates.
- SLB Viewer: This role can only visualize the TOE information and load balancing statistics but cannot make any configuration changes.

- SLB Operator: This role extends the SLB viewer and Operator roles by gaining the functionality to enable or disable physical ports.
- SLB Administrator: This role has complete administrative access to all functionality related to the virtual service configuration, including managing virtual servers, SSL policies, managing back end servers, and other related functionality. However, it does not have access to the rest of the TOE management capabilities.
- L4 Administrator: This role extends the SLB administrator role by adding access to SLB filters and bandwidth management.
- L4 Operator: This role has the same access level as the SLB Operator.

The TOE also provides an intrinsic user for the following roles:

- Administrator (admin)
- Operator (oper)
- User (user)
- L4 Administrator (l4admin)
- L4 Operator (l4oper)
- SLB Administrator (slbadmin)
- SLB Operator (slboper)
- SLB Viewer (slbview)

These intrinsic users are not counted as a normal user, and therefore do not have most of the attributes of normal users and are not managed in the same way. Instead, by default, all of the intrinsic users have their own username as password and only the administrator role can change their associated credentials (per intrinsic user).

As outlined, only the users (and the intrinsic user) with the administrator role are capable of accessing the TOE user management configuration. Meanwhile, changes to the core load balancing configuration is available only to select roles (administrators are the only role able to create and alter virtual services, while other administrator roles such as L4/SLB admins cannot manage services but can manage virtual servers and the parameters affecting the load balancing capabilities) thus preventing unauthorized changes to the information flow policy. Nonetheless, all available roles in the TOE have been listed for the sake of completeness.

TOE Security Functional Requirements covered: FMT_MSA.1, FMT_MSA.3, FMT_SMF.1, FMT_SMR.2.

8.1.6 PROTECTION OF THE TSF

The TOE is capable of maintaining time consistency regardless of being deployed as a virtual appliance or on top of a physical appliance. The TOE uses this time tracking to implement proper audit logging for all TSF-relevant events.

TOE Security Functional Requirements covered: FPT_STM.1.

8.1.7 TOE ACCESS

As part of the security mechanism to protect the administrative accounts, the TOE implements configurable session termination. Be it by manually requesting the termination, or by configuring the activity timeout for automatic session termination. The automatic activity timeout is only available to the TOE administrators.

TOE Security Functional Requirements covered: FTA_SSL.3, FTA_SSL.4.

8.1.8 TRUSTED PATH/CHANNELS

In order to provide the secure communications as part of the core load balancing capabilities, the TOE implements secure transport channels via the HTTPS/TLS protocols. These protocols are used during nominal operation of the TOE when communicating with:


- The TOE administrators initiate the communication via the Web Management interface (HTTPS).
- The Virtual Service clients initiate the communication via the data path (Ingress Port). In this case the TOE receive the request from another trusted IT product during load balancing.
- The backend servers initiate the communication via the data path (Egress Port). In this case the TOE redirect the request to the backend servers during load balancing.

TOE Security Functional Requirements covered: FTP_ITC.1, FTP_TRP.1.

8.2 FUNCTIONALITY OUTSIDE OF THE SCOPE

The following TOE functionality falls outside of the scope of the evaluation and will not be evaluated:

- ➔ Server health checks
- ➔ Application SLA Assurance implementing the high availability and clustering capabilities.
- ➔ Web Performance Optimization implementing optimization technologies with FastView.

- 
- Application SLA Monitoring implementing advanced monitoring and application performance metrics.
 - Application Firewall implementing an application layer firewall capabilities with AppWall.
 - Layered Security Architecture implementing additional security features.
 - Review Logs Stored in the TOE

8.2.1.1 OPTIONAL SYSLOG

The TOE has the capability to export the audit events to external syslog servers. This functionality is optional and in order to use it the administrator must have a syslog server on the management network. The syslog support is not part of the TSF, and its usage does not impact the internal storage capabilities of the TOE.

The TOE can be configured to use both, the BSD (RFC3164) or the IETF (RFC5424) formats. And additionally, it can be configured to use syslog on top of TLS, thus providing support for the different syslog server configurations.

Recommendations are included in the Alteon Common Criteria Guide.

9. Acronyms

Acronym	Meaning
ADC	Application Delivery Controller
AMS	Attack Mitigation System
APM	Application Performance Monitoring
CC	Common Criteria
CBC	Cipher Block Chaining+
DH	Diffie-Hellman
DSA	Digital Signature Algorithm
ECDH	Elliptic Curve Diffie Hellman
ECDSA	Elliptic Curve Digital Signature Algorithm
GCM	Galois Counter Mode
HTTPS	HyperText Transfer Protocol Secure
IP	Internet Protocol
NFV	Network Functions Virtualization
NIST	National Institute of Standards and Technology
RSA	Rivest Shamir Adleman Algorithm
SHA	Secure Hash Algorithm
SLA	Service Level Agreement
SLB	Server Load Balancing
ST	Security Target
TLS	Transport Layer Security
TOE	Target of Evaluation
TSS	TOE Summary Specification
VM	Virtual Machine
VA	Virtual Appliance

10. References

[CEM]	Common Criteria for Information Technology Security Evaluation. Evaluation Methodology Version 3.1 Revision 5
[CC]	Common Criteria for Information Technology Security Evaluation. Part 1, 2 and 3 Version 3.1, Revision 5
[SOGIS-ACM]	SOG-IS Crypto Evaluation Scheme Agreed Cryptographic Mechanisms, Version 1.2
[RFC5246]	The Transport Layer Security (TLS) Protocol Version 1.2
[RFC2818]	HTTP Over TLS
[RFC5288]	AES Galois Counter Mode (GCM) Cipher Suites for TLS
[RFC5289]	TLS Elliptic Curve Cipher Suites with SHA-256/384 and AES Galois Counter Mode (GCM)
[RFC8446]	The Transport Layer Security (TLS) Protocol Version 1.3
[RFC3164]	The BSD syslog Protocol
[RFC5424]	The Syslog Protocol

North America

Radware Inc.

575 Corporate Drive

Mahwah, NJ 07430

Tel: +1-888-234-5763

International

Radware Ltd.

22 Raoul Wallenberg St.

Tel Aviv 69710, Israel

Tel: 972 3 766 8666

© 2022 Radware, Ltd. All Rights Reserved. Radware and all other Radware product and service names are registered trademarks of Radware in the U.S. and other countries. All other trademarks and names are the property of their respective owners. Printed in the U.S.A.