Common Criteria Security Target for Hillstone SG-6000 A-Series NGFW and StoneOS 5.5R9

Document Version: 1.1

Date: 09.09.2022

Hillstone™
NETWORKS

Document Control Information

Version	Date	Summary of Changes
0.1	2021-10-19	First version of the Security Target
0.2	2021-10-22	Updates in definition of SFRs
0.4	2021-11-01	Version used with the CC application form
0.5	2021-11-17	Updated list of threats
0.6	2021-12-22	Updated after initial evaluation round
0.7	2021-12-22	Updated headings versions
0.8	2022-01-28	Updates in user security actions
0.9	2022-03-07	General updates
1.0	2022-07-12	Updates in software version for the TOE
1.1	2022-09-09	Updates in guidance version

Abbreviations

Abbreviation	Description
3DES	Triple DES
AAA	Authentication Authorization Accounting
ABD	Abnormal Behavior Detection
AD	Active Directory
AES	Advanced Encryption Standard
AMI	Amazon Machine Image
ATA	Advanced Technology Attachment
ATD	Advanced Threat Detection engine
AV	Anti-Virus
CA	Certificate Authority
CC	Common Criteria for Information Technology Security Evaluation
C&C	Command-and-Control
CLI	Command Line Interface
DEP	Data Execution Protection
DES	Data Encryption Standard
DC	Digital Certificate
DDNS	Dynamic DNS
DGA	Domain Generation Algorithm
DNS	Domain Name System
DSA	Digital Signature Algorithm
EC2	Elastic Compute Cloud
EPP	End Point Protection
EAL	Evaluation Assurance Level
FTP	File Transfer Protocol

Abbreviation	Description
FIPS PUB	Federal Information Processing Standards Publications
GUI	Graphical User Interface
HTTP	Hyper-Text Transport Protocol
HTTPS	Hyper-Text Transport Protocol Secure
IETF	Internet Engineering Task Force
IKE	Internet Key Exchange
iNGFW	intelligent Next-Generation Firewall
IPS	Intrusion Prevention System
IPsec	Internet Protocol Security
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
ISP	Internet Service Provider
KVM	Kernel-based Virtual Machine
L2TP	Layer 2 Tunneling Protocol
LAC	L2TP Access Concentrator
LDAP	Lightweight Directory Access Protocol
LNS	L2TP Network Server
MD5	Message Digest version 5
NETBIOS	Network Basic Input/Output System
NAT	Network Address Translation
NFV	Network Function Virtualization
NGFW	Next Generation Firewall
NIST SP	National Institute of Standards and Technology Special Publications
NTP	Network Time Protocol
PATA	Parallel ATA
PBR	Policy-Based Route
PKC	Public Key Cryptography
PKI	Public Key Infrastructure
POP	Post Office Protocol
PPP	Point-to-Point Protocol
PPPoE	PPP over Ethernet
QEMU	Quick EMUlator
QoS	Quality of Service
QR	Quick Response
RA	Registration Authority
RADIUS	Remote Authentication Dial-In User Service
RDBMS	Relation database management system
RSA	Rivest-Shamir-Adleman
SATA	Serial ATA
SCSI	Small Computer System Interface
SF	Security Function
SFR	Security Functional Requirement
SFP	Security Function Policy
SHA	Secure Hash Algorithm
SMS	Short Message Service

Abbreviation	Description
SMTP	Simple Mail Transfer Protocol
SQL	Structured Query Language
SSH	Secure Shell
SSO	Single Sign-On
SSL	Secure Socket Layer
TACACS	Terminal Access Controller Access Control System
TCP	Transmission Control Protocol
TCP RST	TCP reset
Telnet	TELetype NETwork
TLS	Transport Layer Security
TOE	Target of Evaluation
TSF	TOE Security Functionality
URL	Uniform Resource Locator

DEFINITIONS

Definition	Description
AMI (AWS)	AMI is a special type of virtual appliance that is used to create a VM within the Amazon Elastic Compute Cloud (“EC2”). It serves as the basic unit of deployment for services delivered using EC2. AWS provides on-demand cloud computing platforms and API’s. These cloud computing web services provide a set of primitive abstract technical infrastructure and distributed computing building blocks and tools, like EC2.
bridge-utils	The bridge-utils package contains a utility needed to create and manage bridge devices.
Egress Traffic	Any data or traffic bound for an external entity and passing through the edge router of the host network to reach its destination node.
Ingress Traffic	Composed of all data communications and network traffic originating from external networks and destined for a node in the host network.
KVM	Open source virtualization technology built into Linux. KVM can turn Linux into a hypervisor that allows a host machine to run multiple, isolated virtual environments called guests or VMs.
L2TP	Tunneling protocol used to support VPNs or as part of the delivery of services by ISPs.
libvirt	The libvirt package is a C toolkit to interact with the virtualization capabilities of recent versions of Linux (and other OSes).
MYSQL	Open-source RDBMS.
MSSQL	RDBMS developed by Microsoft.
NETBIOS	Provides services related to the session layer of the OSI model allowing applications on separate computers to communicate over a local area network.
PKI	System that provides public key encryption and digital signature service. PKI is designed to automate secret key and certificate management, and assure the confidentiality, integrity and non-repudiation of data transmitted over the Internet. The certificate of PKI is managed by a public key by binding the public key with a respective user identity by a trusted third-party, thus authenticating the user over the Internet. A PKI system consists of PKC, CA, RA, DC, and related PKI storage library.

Definition	Description
POP3	POP is an application-layer internet standard protocol used by e-mail clients to retrieve e-mail from a mail server, where POP3 is the version in common use.
QEMU	Generic and open source machine emulator and virtualizer.
SSL/TLS	Protocol that guarantees privacy and data integrity between client/server applications communicating over the Internet.
Telnet	Protocol used on the Internet or local area network to provide a bidirectional interactive text-oriented communication facility using a virtual terminal connection.
TSF	Combined functionality of all hardware, software, and firmware of a TOE that must be relied upon for the correct enforcement of the SFRs.
uml-utilities	The uml-utilities package is a port of the Linux kernel to its own system call interface.
UNIX	Family of multitasking, multiuser computer operating systems.
Xen Project	Type-1 hypervisor, providing services that allow multiple computer operating systems to execute the same computer hardware concurrently.
XenServer	Xen can be shipped in a dedicated virtualization platform, such as Citrix Hypervisor (formerly Citrix XenServer).

Notations and Formatting

The notations and formatting used in this ST are consistent with version 3.1 Revision 5 of the Common Criteria (CC).

The **refinement** operation is used to add detail to a requirement, and thus further restricts a requirement. Refinement of security requirements is denoted by **bold text**. Deleted words are denoted by ~~strike-through text~~.

The **selection** operation is used to select one or more options provided by the CC in stating a requirement. Selections are denoted by *italicized* text in square brackets, [*Selection value*].

The **assignment** operation is used to assign a specific value to an unspecified parameter, such as the length of a password. Assignment is indicated by showing the value with bold face in square brackets, [**Assignment_value**].

The **iteration** operation is used when a component is repeated with varying operations. Iteration is denoted by showing the iteration number in parenthesis following the component identifier, (iteration_number).

Assets: Assets to be protected by the TOE are given names beginning with "AS." – e.g. AS.CLASSIFIED_INFO.

Assumptions: TOE security environment assumptions are given names beginning with "A."- e.g., A.Security_Procedures.

Threats: Threat agents are given names beginning with "TA." – e.g., TA.User. Threats to the TOE are given names beginning with "TT." – e.g., TT.Filter_Fails. TOE security environment threats are given names beginning with "TE."-- e.g., TE.Crypto_Fails.

Policies: TOE security environment policies are given names beginning with "P."—e.g., P.Information_AC.

Objectives: Security objectives for the TOE and the TOE environment are given names beginning with "O." and "OE.", respectively, - e.g., O.Filter-msg and OE.Clearance.

1 Security Target Introduction

1.1 ST reference

1.1.1 ST Identification

Common Criteria Security Target for Hillstone SG-6000 A-Series NGFW and StoneOS 5.5R9.

1.1.2 ST version

1.1

1.1.3 ST date

September 9, 2022

1.2 TOE reference

1.2.1 TOE identification

Hillstone SG-6000 A-Series NGFW and StoneOS 5.5R9

1.2.2 TOE hardware version

Refer to section 1.4.

1.2.3 TOE software version

StoneOS 5.5R9, software build version FR25098-YS-V6-r0614

1.2.4 User guidance version

Guidance document	**Version**
Hillstone SG-6000 A-Series Hardware Reference Guide	Version 1.0, 30.11.2021
StoneOS CLI User Guide A Series	Version 5.5R9, 20.10.2021
StoneOS WebUI Guide A Series	Version 5.5R9, 20.10.2021

1.3 Product Overview

A Hillstone NGFW appliance is a network security device that protects a network by controlling the traffic that comes in and out of that network, allowing or denying the data packet by identifying whether it matches the policy rules or not. Besides security functions, a Hillstone NGFW appliance can also works as a bridging device to connect a trust zone (internal network) and untrust zone (external network).

The Hillstone A-Series Next Generation Firewall (NGFW) deploys perimeter protection and provides comprehensive and granular visibility and control of applications and identifies and prevents potential threats associated with high-risk applications.

The TOE is a firewall system composed of a hardware (A-Series) and a software (StoneOS) running within the platform as a whole system.

1.3.1 Product main features

Hillstone solutions can detect and mitigate sophisticated and rapidly evolving ransomware variants at any or all attack stages, including post breach. The following table summarizes the most security-relevant service features common for all Hillstone firewall appliances. For the security features in the scope of the TOE, please refer to section 1.4.3.

Feature	Description
Application Identification and Control	Hillstone NGFW is optimized for content analysis of Layer 7 applications, providing fine-grained control of web applications regardless of port, protocol, or evasive action. It can identify and prevent potential threats associated with high-risk applications while providing policy-based control over applications, users, and user-groups. Security Policies can be defined that guaranteed bandwidth to mission-critical applications while restricting or blocking unauthorized or malicious applications.
Attack Defense	Hillstone NGFW can detect various types of network attacks and take appropriate actions to protect the Intranet against malicious attacks, thus assuring the normal operation of the Intranet and systems.
Firewall	Hillstone NGFW protects a network by controlling the traffic that comes in and out of that network. The basic mechanism of how a firewall works is that allowing or denying the data packet by identifying whether it matches the policy rules or not. Besides security functions, a firewall can also work as a bridging device to connect a trust zone (internal network) and untrust zone (external network).
High Availability	Hillstone NGFW provides high availability, a fail-over solution for communications lines or device failure to ensure the smooth communication and effectively improve the reliability of the network.
IP Reputation	Hillstone NGFW retrieves the risk IP (such as Botnet, Spam, Tor nodes, Compromised, Brute-force) list from the Perimeter Traffic Filtering signature database. It can filter the perimeter traffic based on known risk IP list, and take logging/block action on the malicious traffic that hits the risk IP list.
Intrusion Prevention	Hillstone NGFW can detect and protect mainstream application layer protocols (DNS, FTP, POP3, SMTP, TELNET, MYSQL, MSSQL, ORACLE, NETBIOS), against web-based attacks and common Trojan attacks.
IPv6	This enables features based on IPv6.
Log	Log is a feature that records various kinds of system logs, including device log, threat log, session log, NAT log, File filter log, Network Behavior Record logshare access logs, and URL logs.
Report	Through gathering and analyzing the device traffic data, traffic management data, threat data, monitor data and device resource utilization data, the function provides the all-around and multi-dimensional statistics.

Feature	Description
URL Filtering	URL filtering controls the access to some certain websites and records log messages for the access actions. URL filtering helps you control the network behaviors in the following access control aspects: Access control to certain category of websites, such as gambling and pornographic websites. Access control to certain category of websites during the specified period. For example, forbid to access IM websites during the office hours. Access control to the website where the URL contains the specified keywords. For example, forbid to access the URL that contains the keyword of game.
User Authentication	When a security product enables authentication, the users and hosts can be denied or allowed to access certain networks.
Virus Filtering	With this function configured, Hillstone devices can detect various threats including worms, Trojans, malware, malicious websites, and proceed with the configured actions.
VPN	System supports the following VPN functions: "IPsec VPN": IPsec is a security framework defined by the Internet Engineering Task Force (IETF) for securing IP communications. It is a Layer 3 virtual private network (VPN) technology that transmits data in a secure tunnel established between two endpoints. "SSL VPN": SSL provides secure connection services for TCP-based application layer protocols by using data encryption, identity authentication, and integrity authentication mechanisms. "L2TP over IPsec VPN": L2TP is one protocol for VPDN tunneling. VPDN technology uses a tunneling protocol to build secure VPNs for enterprises across public networks. Branch offices and traveling staff can remotely access the headquarters' Intranet resources through a virtual tunnel over public networks.
Botnet C&C	Hillstone's advanced Botnet C&C prevention feature prevents communication to the control channel, and detect and block bots within the intranet as well.
Cloud Sandbox	A cloud sandbox provides sophisticated detection and prevention of malicious files through static analysis and pre-processing, followed by behavioral analysis that includes detection of evasive maneuvers. Cloud intelligence then identifies and blocks malicious files, generates logs and reports, and shares threat intelligence back to the cloud.
Antispam	Anti-spam provides real-time spam classification and prevention for both inbound and outbound traffic.

Table 1: Hillstone security-relevant features

1.4 TOE Description

This section provides an overview of the Hillstone Next Generation Firewall appliances Target of Evaluation (TOE). The TOE is comprised of both hardware and software.

The hardware is comprised of the following: A-Series appliances:

- SG-6000-A200
- SG-6000-A200W
- SG-6000-A1000;
- SG-6000-A1100;
- SG-6000-A2000;
- SG-6000-A2600;
- SG-6000-A2700;
- SG-6000-A2800;
- SG-6000-A3000;
- SG-6000-A3600;
- SG-6000-A3700;
- SG-6000-A3800.
- SG-6000-A5100
- SG-6000-A5200;
- SG-6000-A5500;
- SG-6000-A5600;
- SG-6000-A5800.
- SG-6000-A6800
- SG-6000-A7600

The A-Series appliances have common hardware characteristics within each of the models. These differing characteristics affect only non-TSF relevant functionality (such as throughput, processing speed, number and type of network connections supported, number of concurrent connections supported, and amount of storage) and therefore support security equivalency of the appliances in terms of hardware.

The software is comprised of the operating system StoneOS with software version 5.5R9. The StoneOS software is stored in the firmware of each of the hardware appliances.

The StoneOS system architecture is constituted by:

- Zones, dividing network into multiple segments.
- Interface, the inlet and outlet for traffic going through security zones.
- Policy, which is used to control the traffic flow in security zones/segments.

1.4.1 TOE evaluated configuration and deployment

The physical models of the TOE are specified in section 1.4.2 below, and consist of one or more Hillstone firewall appliances, (including the StoneOS 5.5R9 software). Each instantiation of the physical TOE has two or more network interfaces and can filter IP traffic to and through those interfaces.

The TOE can optionally connect to an NTP server for clock updates, where NTP can be configured with authentication. If the StoneOS is to be remotely administered, the management station can connect using SSH or HTTPS. A syslog server can also be used to store audit records to a syslog server for UNIX or Windows, and the syslog server must support syslog over SSL/TLS. The TOE can filter connections to/from these external servers, including authentication servers, using its IP traffic filtering and can encrypt traffic where necessary using SSL/TLS and/or IPsec.

Use of Telnet protocol is not permitted in the evaluated configuration of the TOE, since Telnet is deemed to have known security issues. Also **usage of HTTP is not permitted** in the evaluation configuration of the TOE.

The following sections provide visual depictions of deployment scenarios for both the physical and the virtual models of TOE. The TOE boundary is surrounded with a red line.

1.4.1.1 Transparent mode deployment

Transparent mode is also known as bridge mode or transparent bridging mode. Under normal circumstances, the firewall in transparent mode is deployed between the router and the switch of the protected network, see figure below, (or it is installed between the Internet and a company's router). The internal network uses its old router to access the Internet, and the firewall only provides security control features.

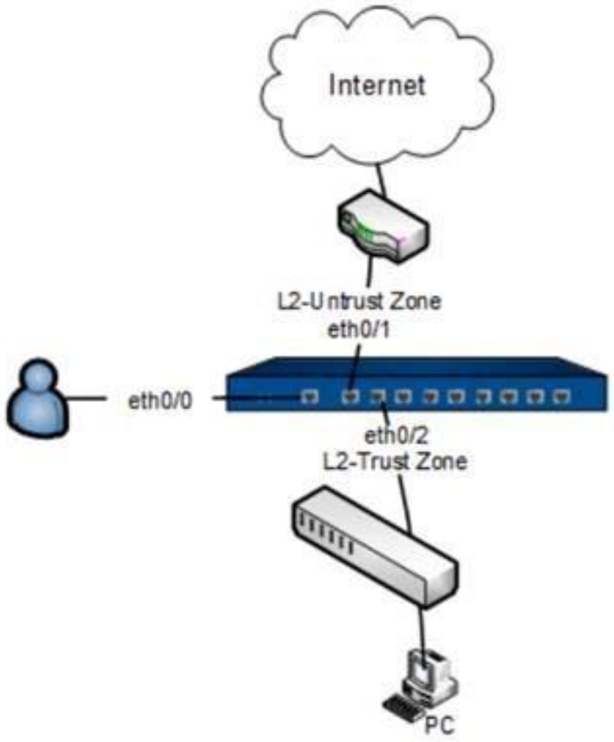


Figure 1: Transparent mode - HW

The administrator uses eth0/0 to manage firewall. The firewall's eth0/1 is connected to router (which is connecting to the Internet), and eth0/2 is connected to a switch (which is connecting to the internal network).

Transparent mode is used when the IT administrator does not wish to change the existing network layout. Normally, the existing network has already set up routers and switches. The firewall will be used as a security device, and the transparent mode has the following advantages:

- No need to change IP addresses
- No need to set up NAT rule

1.4.1.2 Routing mode deployment

Routing mode is mostly used when the firewall is installed between an internal network and the Internet, see figure below.

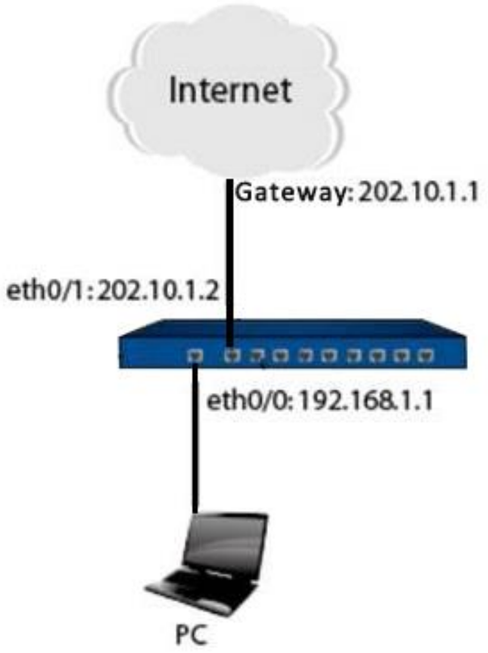


Figure 2: Routing mode - HW

The device connects a private network to the Internet.

Routing mode deployment often uses the NAT function, so it is also called NAT mode. In routing mode, each interface has its IP address which means interfaces are in the layer 3 zone. A firewall in routing mode can work as a router and a security device.

1.4.1.3 Mix mode deployment

If the firewall has both L2 interfaces (transparent mode) and L3 interfaces (routing mode), the firewall is in mix mode, see figure below.

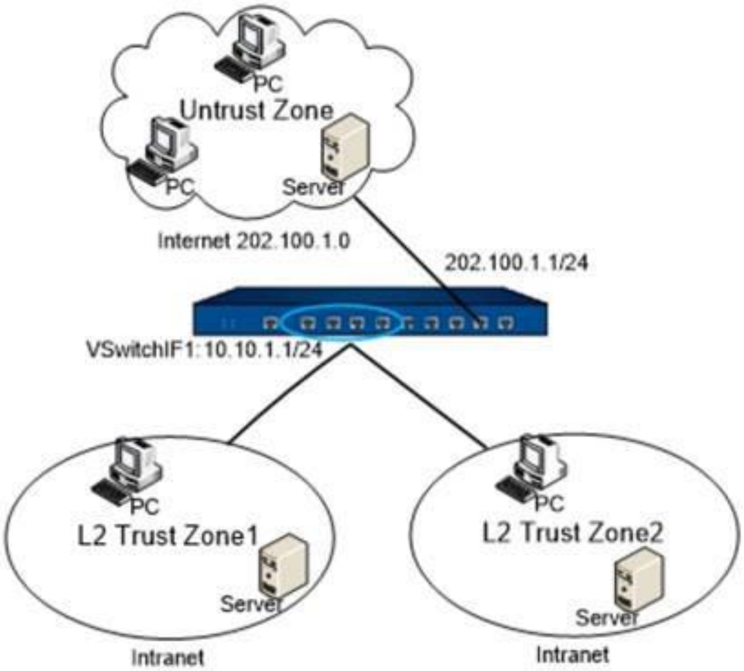


Figure 3: Mix mode - HW

To configure a mix mode, it is necessary to combine the routing mode of the deployment methods with the transparent mode.

1.4.2 TOE Physical scope

The TOE is a hardware and software solution comprised of NGFW appliance models. The Hillstone hardware appliances are outlined in the table below.

All the following models share the same OS, the StoneOS 5.5R9.

<table>
<tr><th>TOE Configuration</th><th>Guidance</th></tr>
<tr><td>All product families in scope</td><td>
<table>
<tr><th>Guidance document</th><th>Version</th></tr>
<tr><td>Hillstone SG-6000 A-Series Hardware Reference Guide</td><td>Version 1.0, 30.11.2021</td></tr>
<tr><td>StoneOS CLI User Guide A Series</td><td>Version 5.5R9, 20.10.2021</td></tr>
<tr><td>StoneOS WebUI Guide A Series</td><td>Version 5.5R9, 20.10.2021</td></tr>
</table>
</td></tr>
</table>

Table 2: TOE Identification of Desktop Models

1.4.3 TOE Logical scope

All the hardware models share the same OS, the StoneOS 5.5R9. The OS is installed and run on the physical TOE.

The Hillstone Next Generation Firewall TOE is comprised of several security features, all implemented by StoneOS:

1. Security Audit
2. Cryptographic Support
3. User Data Protection
4. Identification and Authentication
5. Security Management
6. Protection of the TSF
7. Trusted Path/Channels

Each of the security features identified consists of several security functionalities, as identified below.

NOTE: A TOE administrative user, which must be identified and authenticated in order to manage the TOE, will from now on be denoted as "TOE administrator" or "administrator". (The term "authorized administrator" is used throughout this ST to describe an administrator given the appropriate permission to perform tasks as required). A TOE end user, which may be required to authenticate in order to access an internal or external network, will from now on be denoted as "TOE user" or "user".

1.4.3.1 Security Audit

The TOE provides extensive auditing capabilities by generating an audit record for each auditable even, thus generating a comprehensive set audit logs that identify specific TOE operations including audit records for security relevant events.

The TOE can audit events related to identification and authentication, and administrative actions.

The administrator may view the contents of the audit records, and for each event, the TOE records the date and time of each event, the type of event, the subject identity, and the outcome of the event.

1.4.3.2 Cryptographic Support

The TOE provides cryptography in support of other Hillstone appliance security functionality. The TOE provides cryptography in support of VPN connections using IPsec and SSL/TLS, and remote administrative management via SSH and HTTPS.

The TOE provides key generation, key destruction and cryptographic operation functions supported by algorithms.

1.4.3.3 User Data Protection

The TOE provides interfaces to a defined set of networks and mediates information flow among these networks. The TOE supports the information flow control policies required for authenticated and unauthenticated service. Additionally, the TOE supports a VPN information flow control policy and a Web filtering information flow control policy.

1.4.3.4 Identification and Authentication

All TOE administrators must be identified and authenticated. Administration may either be performed locally using the local Console CLI or remotely using the network Web-based GUI, supported by an IPsec protected AAA server. Hillstone NGFW has four administrator roles: admin, admin-read-only, operator, and auditor.

TOE users may be required to authenticate in order to access an internal or external network. If the administrator configure authentication, the users can be authenticated via Web Authentication or VPN, supported by an AAA server.

1.4.3.5 Security Management

The TOE provides secure administrative services for management of general TOE configuration and the security functionality provided by the TOE. All TOE administration occurs either via a local Console connection, or through a secure SSH or HTTPS session.

The TOE provides the ability to manage all TOE administrators, all identification and authentication, all audit functionality of the TOE, all TOE cryptographic functionality, and the information flow control policies enforced by the TOE including encryption/decryption of information flows for VPNs.

TOE administrators of different roles have different privileges, and the TOE supports pre-defined administrator roles and customized administrator roles. By default, the system supports the following administrator roles, which cannot be deleted or edited: admin, admin-read-only, operator, and auditor. The administrator role "admin" has permission for reading, executing, and writing, has the authority over all features, and can view the current or historical configuration information.

1.4.3.6 Protection of the TSF

The TOE protects against interference and tampering by untrusted subjects by implementing identification, authentication, and access controls to limit configuration to authorized administrators.

The TOE internally maintains the date and time. This date and time are used as the timestamp that is applied to audit records generated by the TOE. Administrators can configure the current system time manually or synchronize the system time with the NTP server time via NTP protocol, where NTP can be configured with authentication (appends cryptographic signature to each network packet) to ensure that received NTP packets originates from NTP servers. Additionally, the TOE performs testing by means of DNS Query, Ping and Traceroute verify correct operation of the TOE.

1.4.3.7 Trusted Path/Channels

The TOE supports establishing trusted paths between itself and remote administrators using SSH for CLI access and HTTPS for GUI access. The TOE supports use of SSL/TLS and/or IPsec for connections with remote syslog servers. The TOE supports IPsec to encrypt connections with remote authentication servers (RADIUS or TACACS+). The TOE supports IPsec to encrypt connections with NTP servers.

1.4.4 Optional non-TOE components

The TOE can be used to connect to the following external servers:

- Syslog, authentication, and NTP.

These external servers are optional for the functionality of the TOE, therefore not in the scope of the evaluation.

2 Conformance Claims

This TOE and ST are conformant with the following specifications.

Item	Identification
Part 2 of the ISO/IEC 15408 international standard	Common Criteria security functional components, April 2017, Version 3.1, Revision 5, conformant

Item	Identification
Part 3 of the ISO/IEC 15408 international standard	Common Criteria security assurance components, April 2017, Version 3.1, Revision 5, conformant
Extended SFRs	None
Protection Profiles	None
Packages	EAL4, augmented with ALC_FLR.1

Table 3: Conformance Claims

3 Security Problem Definition

This chapter identifies the following:

- IT related threats to the organization countered by the TOE.
- Organizational security policies for the TOE as appropriate.
- Significant assumptions about the TOE's operational environment.

3.1 Threats to security

3.1.1 Assets

Assets	Description
AS.DATA	Sensitive or security TOE functionality data (TSF data), either contained in the TOE storage or moved from the TOE storage to a remote storage system.
AS.KEY	Cryptographic keys contained in the TOE, for encryption of data in flight.
AS.INTERNAL NETWORK	Data residing on servers or workstations present on the internal network which is protected by the firewall against unauthorized external access

Table 4: TOE Assets

3.1.2 Threat Agents

Threat Agents	Description
TA.ATTACKER	A person/company or process (IT entity) with skills and resources to mislead the system in any way necessary to reveal/divulge/misuse data and prevent the system from operating.
TA.ADMIN	Authorized person or process (IT entity) that performs installation and configuration/setup of the TOE to ensure that the TOE operates according to the needs of the target network system.
TA.USER	Authorized person or process (IT entity) who may unintentionally perform unauthorized actions.

Table 5: Threat Agents for TOE

3.1.3 Identification of Threats

3.1.3.1 Threats to the TOE

The following table lists the threats addressed by the TOE. The assumed level of expertise of the attacker for all the threats identified below is Enhanced-Basic.

Threats in scope of the TOE	Description
TT.ADMIN_ERROR	The admin incorrectly configures the TOE, which results in potential compromise of TSF data due to ineffective security mechanisms deployed.
Threat agents:	TA.ADMIN

Threats in scope of the TOE	Description
Assets:	AS.DATA
Attack method:	During operation, the administrator unintentionally configures the TOE incorrectly, making the TOE inoperable or resulting in ineffective security mechanisms.
TT.ADMIN_EXPLOIT	An external malicious attacker gain access to an administrator account by means of external hacking into the product, therefore getting access to sensitive TSF data.
Threat agents:	TA.ATTACKER
Assets:	AS.DATA
Attack method:	A person/company uses hacking methods to exploit missing, weak, or incorrectly implemented access control in the TOE.
TT_AUDIT_COMPROMISE	An external malicious attacker modifies or removes audit records (TSF data) to mask actions in the past or prevent logging of actions in the future, by means of external hacking into the TOE.
Threat agents:	TA.ATTACKER
Assets:	AS.DATA
Attack method:	A person/company uses hacking methods to exploit weakness in the TOE.
TT.CRYPTO_ COMPROMISE	An external malicious attacker compromises the cryptographic keys used by the TOE, by means of and external attack.
Threat agents:	TA.ATTACKER
Assets:	AS.KEY
Attack method:	An attacker cause keys associated with the cryptographic functionality to be inappropriately accessed (viewed/modified/deleted), thus compromising the cryptographic mechanisms protected by those mechanisms.
TT.HACK_ACCESS	An external malicious attacker gets undetected system access to the TOE and therefore accesses TSF data, due to missing, weak and/or incorrectly implemented access control, causing potential violations of integrity, confidentiality, or availability.
Threat agents:	TA.ATTACKER
Assets:	AS.DATA
Attack method:	A person/company uses hacking methods to exploit missing, weak, or incorrectly implemented access control in the TOE.

Threats in scope of the TOE	Description
TT.NETWORK_ACCESS	An external malicious attacker gets access to the internal network protected by the firewall by defeating the authentication to the TOE and defeating the firewall policy rules. In this way, the external attacker can cause violations of the integrity, confidentiality of availability of data present on the protected internal network.
Threat agents:	TA.ATTACKER
Assets:	AS.INTERNAL NETWORK
Attack method:	A person/company uses hacking methods to defeat the TOE's user authentication and firewall policies.

Table 6: Security Threats

3.1.3.2 Threats to the TOE Environment

Not applicable.

3.2 Organizational Security Policies (OSP)

The following table lists the Organizational Security Policies imposed by an organization to address its security needs.

Organizational security Policies	Description
P.ACCOUNTABILITY	The authorized administrators and users of the TOE shall be held accountable for their actions.
P.ADMIN_ACCESS	An authorized administrator must manage the TOE securely.
P.DETECT	In order to trace all security-related responsibilities, security-related events shall be documented, maintained, and analyzed, and such records can be checked.

Table 7: Organizational security Policies

3.3 Assumptions

The specific conditions listed in the following table are assumed to exist in the TOE's environment. These assumptions include both practical realities in the development of the TOE security requirements and the essential environmental conditions on the use of the TOE.

Assumptions	Description
A.NO_GENERAL_PURPOSE	There are no general-purpose computing capabilities (e.g., compilers or applications) available on the TOE, other than those services necessary for the operation, administration, and support of the TOE.
A.PHYSICAL	The TOE shall presumably be located in physically secure environment that can be accessed only by the authorized administrators.

Assumptions	Description
A.TRUSTED_ADMIN	The administrators of the TOE shall not have any malicious intention, shall receive proper training on the TOE management, and shall follow the administrator guidelines.

Table 8: TOE Environment Assumptions

4 Security Objectives

This chapter defines the security objectives for the TOE and its supporting environment. The security objectives are intended to counter identified threats, comply with defined organizational security policies, and address applicable assumptions.

4.1 TOE Security Objectives

This section defines the security objectives that are to be addressed by the TOE.

Security Objectives	Description
O.ACCESS	The TOE must allow only authorized administrators to access only appropriate TOE functions and data.
O.AUDIT	The TOE shall record and maintain security-related events associated with administrators and users in order to enable tracing of responsibilities for security-related acts and shall provide means to review the recorded data.
O.CRYPTO	The TOE must protect the confidentiality and integrity of data passed between itself and an authorized administrator, and between itself and the external servers (syslog, authentication, NTP).
O.IDAUTH	The TOE must be able to identify and authenticate authorized administrators prior to allowing access to TOE security management functions. (If required, the TOE must be able to identify and authenticate authorized users prior to allowing access to a connected network).
O.MANAGE	The TOE must include a set of functions that allow effective management of its functions and data. The TOE will provide mechanisms to ensure that only administrators are able to log in and configure the TOE and provide protections for logged-in administrators.
O.MEDIATE	The TOE must mediate the flow of all information between clients and servers located on internal and external networks governed by the TOE.
O.PROTECT	The TOE must protect itself and its resources from unauthorized modifications and access to its functions and data.
O.REUSE	The TOE must provide a means to prevent the reuse of authentication data for users attempting to authenticate to the TOE from a connected network.

Security Objectives	Description
O.TIME	The TOE shall provide reliable time stamps and the capability for the administrator to set the time-source used for these time stamps, in that the administrator can configure the TOE to synchronize its clocks with NTP servers.

Table 9: Security Objectives for the TOE

4.2 Operational Environment Security Objectives

This section defines the security objectives that are to be addressed by the operational environment of the TOE.

Security Objectives	Description
OE.NO_GENERAL_PURPOSE	There are no general-purpose computing capabilities (e.g., compilers or applications) available on the TOE, other than those services necessary for the operation, administration, and support of the TOE.
OE.PHYSICAL	Those responsible for the TOE must ensure that the hardware on which the TOE and OS are installed, is protected from any physical attack.
OE.TRUSTED_ADMIN	The administrator of the TOE shall not have any malicious intention, shall receive proper training on the TOE management, and shall follow the administrator guidelines.

Table 10: Security Objectives for the Operational Environment

4.3 Security Objectives Rationale

The following tracing shows which security objectives address which threats, policies (OSPs) and assumptions.

	Threats						Policies			Assumptions		
	TT.ADMIN_ERROR	TT.ADMIN_EXPLOIT	TT.AUDIT_COMPROMISE	TT.CRYPTO_COMPROMISE	TT.HACK_ACCESS	TT.NETWORK_ACCESS	P.ACCOUNTABILITY	P.ADMIN_ACCESS	P.DETECT	A.NO_GENERAL_PURPOSE	A.PHYSICAL	A.TRUSTED_ADMIN
TOE Security Objectives												
O.ACCESS	X	X	X		X			X				
O.AUDIT			X		X		X		X			
O.CRYPTO					X							
O.IDAUTH		X	X		X		X					
O.MANAGE	X				X			X				

	Threats						Policies			Assumptions		
	TT.ADMIN_ERROR	TT.ADMIN_EXPLOIT	TT.AUDIT_COMPROMISE	TT.CRYPTO_COMPROMISE	TT.HACK_ACCESS	TT.NETWORK_ACCESS	P.ACCOUNTABILITY	P.ADMIN_ACCESS	P.DETECT	A.NO_GENERAL_PURPOSE	A.PHYSICAL	A.TRUSTED_ADMIN
O.MEDIATE					X	X						
O.PROTECT				X	X							
O.REUSE		X			X							
O.TIME							X		X			
Operational Environment Security Objectives												
OE.NO_GENERAL_PURPOSE										X		
OE.PHYSICAL			X								X	
OE.TRUSTED_ADMIN	X	X			X		X	X				X

Table 11: Mapping of Objectives to Threats, Policies and Assumptions

The following table is a set of justifications that shows that all threats, policies (OSPs), and assumptions are effectively addressed by the security objectives.

Threat/Policy/Assumption	Security Objective Rationale
TT.ADMIN_ERROR	The TOE may be incorrectly configured that may result in the TOE's acquisition of ineffective security mechanisms. O.ACCESS and O.MANAGE provide authorized administrators the capability to view and manage configuration settings. OE.TRUSTED_ADMIN ensures that the administrators are non-hostile and are trained to appropriately manage and administer the TOE.
TT.ADMIN_EXPLOIT	A person/company may gain access to an administrator account. O.ACCESS restricts access to administrative functions to the authorized administrators. O.IDAUTH includes mechanisms to authenticate TOE administrators and place controls on administrator sessions. O.REUSE ensures that the TOE provides a means to prevent the reuse of authentication data, providing a means to mitigate the threat of replaying authentication information. OE.TRUSTED_ADMIN ensures that the TOE administrators have guidance that instructs them how to administer the TOE in a secure manner.

Threat/Policy/Assumption	Security Objective Rationale
TT_AUDIT_COMPROMISE	A person/company may modify or remove audit records to mask actions in the past or prevent logging of actions in the future. O.ACCESS requires that administrators shall access only appropriate TOE functions and data. O.AUDIT specifies that management actions are audited, allowing such access to be monitored. O.IDAUTH requires that administrators must be identified and authenticated before access is granted, thus inhibiting unauthorized administrators from gaining access to TOE data. OE.PHYSICAL aims to prevent access to the TOE server appliances by those aiming to access TOE data.
TT.CRYPTO_ COMPROMISE	An attacker may compromise cryptographic keys and the data protected by the cryptographic mechanisms. O.PROTECT ensures that the TOE will have adequate protection from external sources and that all TOE Security Policy functions are invoked.
TT.HACK_ACCESS	A person/company gets undetected system access to the TOE due to missing, weak and/or incorrectly implemented access control, causing potential violations of integrity, confidentiality, or availability. O.ACCESS and O.IDAUTH provide the means to identify and authenticate the TOE administrators. The correct identity of the administrator is the basis for any decision of the TOE about an attempt of an administrator to access data. O.AUDIT provides the TOE the capability to detect and create records of security-relevant events associated with administrators and users. O.CRYPTO ensures the confidentiality and integrity of data passed between the TOE and the authorized administrator for management purposes, and between the TOE and remote servers. O.MANAGE restricts the ability to modify the security attributes associated with access control rules, access to authenticated and unauthenticated services, etc. to the authorized administrators. These objectives ensure that no other administrator can modify the information flow policy to bypass the intended TOE security policy.

Threat/Policy/Assumption	Security Objective Rationale
	O.MEDIATE ensures that all information between clients and servers located on internal and external networks is mediated by the TOE. O.PROTECT ensures that the TOE will have adequate protection from external sources and that all TOE Security Policy functions are invoked. O.REUSE ensures that the TOE provides a means to prevent the reuse of authentication data, providing a means to mitigate the threat of replaying authentication information. OE.TRUSTED_ADMIN ensures that the TOE administrators have guidance that instructs them how to administer the TOE in a secure manner.
TT.NETWORK_ACCESS	An external malicious attacker gets access to the internal network protected by the firewall by defeating the authentication to the TOE and defeating the firewall policy rules. In this way, the external attacker can cause violations of the integrity, confidentiality of availability of data present on the protected internal network. O.MEDIATE ensures that all information between clients and servers located on internal and external networks is mediated by the TOE.
P.ACCOUNTABILITY	The authorized administrators and users of the TOE shall be held accountable for their actions. O.AUDIT provides the administrator with the capability of configuring the audit mechanism to record the actions of a specific user or review the audit trail based on the identity of the user. Additionally, the administrator's user-identifier is recorded when any security relevant change is made to the TOE (e.g. modifying TSF data, login sessions). O.IDAUTH requires the TOE to identify and authenticate administrators prior to allowing any TOE access on behalf of those administrators. O.TIME requires the TOE to provide a reliable time stamp (settable only by the authorized administrator). The audit mechanism is required to include the current date and time in each audit record.

Threat/Policy/Assumption	Security Objective Rationale
	OE.TRUSTED_ADMIN ensures that the TOE administrators have guidance that instructs them how to administer the TOE in a secure manner.
P.ADMIN_ACCESS	An authorized administrator must manage the TOE securely. O.ACCESS and O.MANAGE provide authorized administrators the capability to view and manage configuration settings. OE.TRUSTED_ADMIN ensures that the administrators are non-hostile and are trained to appropriately manage and administer the TOE.
P.DETECT	In order to trace all security-related responsibilities, security-related events shall be documented, maintained, and analyzed, and such records can be checked. O.AUDIT ensures the collection of data on security relevant events. O.TIME ensures that the audit functionality can include reliable timestamps.
A.NO_GENERAL_PURPOSE	There are no general-purpose computing capabilities (e.g., compilers or applications) available on the TOE, other than those services necessary for the operation, administration, and support of the TOE. OE.NO_GENERAL_PURPOSE ensures that there are no general-purpose computing capabilities (e.g., the ability to execute arbitrary code or applications) on the TOE.
A.PHYSICAL	The TOE shall presumably be located in physically secure environment that can be accessed only by the authorized administrators. OE.PHYSICAL ensures that the environment provides physical security, commensurate with the value of the TOE and the data it contains.
A.TRUSTED_ADMIN	The administrators of the TOE shall not have any malicious intention, shall receive proper training on the TOE management, and shall follow the administrator guidelines. OE.TRUSTED_ADMIN ensures that the administrators of the TOE shall not have any malicious intention, shall receive proper training on the TOE management, and shall follow the administrator guidelines.

Table 12: Rationale between Objectives and SPDs

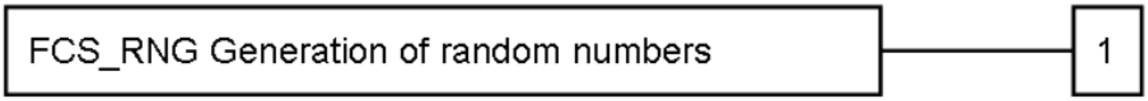
5 Extended Components Definition

If applicable, this chapter defines security components for the TOE not already defined in CC part 2 or CC part 3. The following extended component has been included in this Security Target because the Common Criteria components were found to be insufficient as stated.

5.1 Extended Components

An additional family (FCS_RNG) is defined in this Security Target, in order to provide relevant security functional requirements to the TOE. The family is included within the class FCS (Cryptographic Support), due to the fact that the random numbers are a major component in building up cryptographic algorithms and functions. This additional family describes the functional requirements needed for random number generation. The additional family definition is taken from PP0084[1], a certified Protection Profile used for the evaluation of security IC platforms. As the random number generation function defined by this family is considered sufficient to satisfy the random number generation needs for the TOE, full re-use is made of the FCS_RNG family definition in PP084.

The family contains a single component, FCS_RNG.1.



The definition of the FCS_RNG.1 component, as taken from PP084, is considered for this ST.

FCS_RNG.1	**Random number generation**
Hierarchical to:	No other components
Dependencies	No dependencies
FCS_RNG.1.1	The TSF shall provide a [selection: *physical, non-physical true, deterministic, hybrid physical, hybrid deterministic*] random number generator that implements: [assignment: *list of security capabilities*]

[1] Security IC Platform Protection Profile with Augmentation Packages, Version 1.0

FCS_RNG.1.2	The TSF shall provide [selection: *bits, octets of bits, numbers [assignment: format of the numbers]*] that meet [assignment: *a defined quality metric*]

6 Security Requirements

6.1 Security Functional Requirements (SFRs)

Functional Class	Functional Component	
FAU: Security audit	FAU_GEN.1	Audit data generation
	FAU_GEN.2	User identity association
	FAU_SAR.1	Audit review
	FAU_SAR.2	Restricted audit review
	FAU_SAR.3	Selectable audit review
	FAU_STG.1	Protected audit trail storage
	FAU_STG.3	
FCS: Cryptographic support	FCS_CKM.1(1)	Cryptographic key generation (asymmetric)
	FCS_CKM.1(2)	Cryptographic key generation (symmetric)
	FCS_CKM.4	Cryptographic key destruction
	FCS_COP.1	Cryptographic operation
	FCS_RNG.1	Random number generation
FDP: User Data Protection	FDP_ACC.1	Subset access control
	FDP_ACF.1	Security attribute based access control
	FDP_IFC.1(1)	Subset information flow control (unauthenticated)
	FDP_IFC.1(2)	Subset information flow control (authenticated)
	FDP_IFF.1(1)	Simple security attributes (unauthenticated)
	FDP_IFF.1(2)	Simple security attributes (authenticated)
FIA: Identification and authentication	FIA_ATD.1	User attribute definition
	FIA_UAU.2	User authentication before any action
	FIA_UAU.5	Multiple authentication mechanisms

Functional Class	Functional Component	
	FIA_UID.2	User identification before any action
	FIA_AFL.1	Authentication failure handling
	FIA_SOS.1	Verification of secrets
FMT: Security management	FMT_MOF.1	Management of security functions behaviour
	FMT_MSA.1	Management of security attributes (unauthenticated)
	FMT_MSA.3	Static attribute initialization
	FMT_SMF.1	Specification of Management Functions
	FMT_SMR.1	Security roles
FPT: Protection of the TSF	FPT_STM.1	Reliable time stamps
FTP: Trusted Path/Channels	FTP_ITC.1	Inter-TSF trusted channel
	FTP_TRP.1	Trusted path
FTA: TOE access	FTA_SSL.1	TSF-initiated session locking

Table 13: Security Functional Requirements

6.1.1 Security Audit (FAU)

6.1.1.1 FAU_GEN.1 Audit data generation

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) [**Auditable events listed in Table 14**].

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, [**additional information listed in Table 14**].

Requirement	Auditable Events	Additional Audit Record Contents

FDP_IFF.1(1)
FDP_IFF.1(2)
	Decisions to permit/deny information flows	

FIA_UAU.2	All use of the authentication mechanism	
FIA_UAU.5	Decision of the authentication mechanism	Claimed identity of the user attempting to authenticate (configuration log audit events)
FIA_UID.2	All use of the identification mechanism	
FMT_MOF.1	All modifications in the behavior of the functions in the TSF	

FMT_MSA.1(1)
FMT_MSA.1(2)
	Modification of the security attributes	

FMT_MSA.3(1)
FMT_MSA.3(2)
	Modification to the default settings or initial values of security attributes	

FMT_SMF.1	Use of management functions	
FTP_TRP.1	Failure of the trusted path functions	Identification of the claimed user identity (configuration log audit events)

Table 14: Auditable Events

6.1.1.2 *FAU_GEN.2 User identity association*

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.

6.1.1.3 *FAU_SAR.1 Audit review*

Dependencies: FAU_GEN.1 Audit data generation

FAU_SAR.1.1 The TSF shall provide [**administrators with the roles Administrator, Administrator read-only, and Auditor**] with the capability to read [**all audit information**] from the audit records.

FAU_SAR.1.2 The TSF shall provide the audit records in a manner suitable for the user to interpret the information.

6.1.1.4 *FAU_SAR.2 Restricted audit review*

Dependencies: FAU_SAR.1 Audit review

FAU_SAR.2.1 The TSF shall prohibit all users read access to the audit records, except those users that have been granted explicit read-access.

6.1.1.5 FAU_SAR.3 Selectable audit review

Dependencies: FAU_SAR.1 Audit review

FAU_SAR.3.1 The TSF shall provide the ability to apply [**searches**] of audit data based on [**filter options**].

6.1.1.6 FAU_STG.1 Protected audit trail storage

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.

6.1.1.7 FAU_STG.3 Action in case of possible audit data loss

Dependencies: FAU_STG.1 Protected audit trail storage

FAU_STG.3.1 The TSF shall **[override the earliest data or stop recording data – configurable selection]** if the audit trail exceeds **[90% of storage capacity – configurable option]**

6.1.2 Cryptographic Support (FCS)

6.1.2.1 FCS_CKM.1(1) Cryptographic key generation (asymmetric)

Dependencies: [FCS_CKM.2 Cryptographic key distribution, or
FCS_COP.1 Cryptographic operation]
FCS_CKM.4 Cryptographic key destruction

FCS_CKM.1.1(1) The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [**RSA and DSA**] and specified cryptographic key sizes [**listed in Table 15**] that meet the following: [**FIPS PUB 186-4**].

6.1.2.2 FCS_CKM.1(2) Cryptographic key generation (symmetric)

Dependencies: [FCS_CKM.2 Cryptographic key distribution, or
FCS_COP.1 Cryptographic operation]
FCS_CKM.4 Cryptographic key destruction

FCS_CKM.1.1(2) The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [**Key Derivation Functions using Pseudorandom Function**] and specified cryptographic key sizes [**listed in Table 15**] that meet the following: [**NIST SP 800-135 Revision 1**].

Key Usage		Key Size (bits)
Asymmetric	RSA	2048
	DSA	2048
Symmetric	3DES	192

	AES	128, 192, 256

Table 15: Cryptographic Key Generation

6.1.2.3 FCS_CKM.4 Cryptographic key destruction

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or
FDP_ITC.2 Import of user data with security attributes, or
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 [**zeroization of keys provided by StoneOS**] that meets the following: [**FIPS PUB 140-2**].

6.1.2.4 FCS_COP.1 Cryptographic operation

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or
FDP_ITC.2 Import of user data with security attributes, or
FCS_CKM.1 Cryptographic key generation]
FCS_CKM.4 Cryptographic key destruction

FCS_COP.1.1 The TSF shall perform [**the cryptographic operations specified in Table 16**] in accordance with a specified cryptographic algorithm [**the cryptographic algorithms specified in Table 16**] and cryptographic key sizes [**cryptographic key sizes specified in Table 16**] that meet the following: [**standards listed in Table 16**].

Operation	Algorithm	Key Size or Digest Length (bits)	Standard
Symmetric Encryption/ Decryption	3DES	192	NIST SP 800-67
	AES	128, 192, 256	FIPS PUB 197
Key Exchange	Diffie-Hellman	2048, 3072, 4096	N/A
Hashing	MD5	128	N/A
	SHA	160, 256, 384, 512	FIPS PUB 180-4
HMAC	HMAC-MD5	128	N/A
	HMAC-SHA-1	160	FIPS PUB 198-1
	HMAC-SHA-256	256	FIPS PUB 198-1
	HMAC-SHA-384	384	FIPS PUB 198-1
	HMAC-SHA-512	512	FIPS PUB 198-1
Digital Signature	RSA	2048	FIPS PUB 186-4
	DSA	2048	FIPS PUB 186-4

Table 16: Cryptographic Operations

6.1.2.5 *FCS_RNG.1 Cryptographic operation*

Dependencies: none

FCS_RNG.1.1 The TSF shall provide a [*deterministic*] random number generator that implements: **[generation of random bytes for usage within key generation, SSL/TLS negociation, IKE negociation, calculation of MFA data].**

FCS_RNG.1.2 The TSF shall provide [*octets of bits*] that meet **[random bytes with a probability of 2^8 of occurring]**

6.1.3 User Data Protection (FDP)

6.1.3.1 *FDP_ACC.1 Subset access control*

Dependencies: FDP_ACF.1 Security attribute based access control

FDP_ACC.1.1 The TSF shall enforce the [**Access Control SFP**] on [
Subjects: authorized administrators and users;
Objects: commands/features provided by TOE;
Operations: execute].

6.1.3.2 *FDP_ACF.1 Security attribute based access control*

Dependencies: FDP_ACC.1 Subset access control
FMT_MSA.3 Static attribute initialisation

FDP_ACF.1.1 The TSF shall enforce the [**Access Control SFP**] to objects based on the following: [
Subjects: authorized administrators and users;
Subject attributes: name, password, and role in table 17 for FMT_SMF.1;
Objects: commands/features provided by TOE;
Object attributes: operation in table 17 for FMT_SMF.1].

FDP_ACF.1.2 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [**the TSF shall allow or deny an administrator access to an operation according to the role settings defined in table 17 for FMT_SMF.1**].

FDP_ACF.1.3 The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [**none**].

FDP_ACF.1.4 The TSF shall explicitly deny access of subjects to objects based on the following additional rules: [**none**].

6.1.3.3 *FDP_IFC.1(1) Subset information flow control (unauthenticated)*

Dependencies: FDP_IFF.1 Simple security attributes

FDP_IFC.1.1(1) The TSF shall enforce the [**Unauthenticated Information Flow Control SFP**] on [
Subjects: unauthenticated users and IT entities that send and receive information through the TOE to one another;
Information: network traffic sent through the TOE from one subject to another;
Operations: pass or not information].

6.1.3.4 FDP_IFC.1(2) Subset information flow control (authenticated)

Dependencies: FDP_IFF.1 Simple security attributes

FDP_IFC.1.1(2) The TSF shall enforce the [**Authenticated Information Flow Control SFP**] on [
Subjects: authenticated users and IT entities that send and receive information through the TOE to one another;
Information: network traffic sent through the TOE from one subject to another;
Operations: pass or not pass information].

6.1.3.5 FDP_IFF.1(1) Simple security attributes (unauthenticated)

Dependencies: FDP_IFC.1 Subset information flow control
FMT_MSA.3 Static attribute initialisation

FDP_IFF.1.1(1) The TSF shall enforce the [**Unauthenticated Information Flow Control SFP**] based on the following types of subject and information security attributes: [
Subjects: unauthenticated users and IT entities that send and receive information through the TOE to one another;
Subject security attributes: address;
Information: network traffic sent through the TOE from one subject to another;
Information security attributes:

- **source zone and address of the traffic,**
- **destination zone and address of the traffic,**
- **service type of the traffic].**

FDP_IFF.1.2(1) The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold:
[**Subjects can cause information to flow through the TOE to another connected network if all the information security attribute values are unambiguously permitted by the information flow security policy rules, where such rules may be composed from all possible combinations of the values of the information flow security attributes**].

FDP_IFF.1.3(1) The TSF shall enforce the [**actions that the TOE will perform when processing the specific type of traffic, including Permit, Deny, Tunnel, From tunnel, WebAuth, and Portal server**].

FDP_IFF.1.4(1) The TSF shall explicitly authorise an information flow based on the following rules: [**none**].

FDP_IFF.1.5(1) The TSF shall explicitly deny an information flow based on the following rules: [**none**].

6.1.3.6 FDP_IFF.1(2) Simple security attributes (authenticated)

Dependencies: FDP_IFC.1 Subset information flow control
FMT_MSA.3 Static attribute initialisation

FDP_IFF.1.1(2) The TSF shall enforce the [**Authenticated Information Flow Control SFP**] based on the following types of subject and information security attributes: [
Subjects: authenticated users and IT entities that send and receive information through the TOE to one another;

Subject security attributes:

- **Address (IPv6 supporting),**
- **identity,**
- **role;**

Information: network traffic sent through the TOE from one subject to another;
Information security attributes:

- **source zone and address of the traffic,**
- **destination zone and address of the traffic,**
- **service type of the traffic].**

FDP_IFF.1.2(2) The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold:
[**Subjects can cause information to flow through the TOE to another connected network if all the information security attribute values are unambiguously permitted by the information flow security policy rules, where such rules may be composed from all possible combinations of the values of the information flow security attributes**].

FDP_IFF.1.3(2) The TSF shall enforce the [**actions that the TOE will perform when processing the specific type of traffic, including Permit, Deny, Tunnel, From tunnel, WebAuth, and Portal server**].

FDP_IFF.1.4(2) The TSF shall explicitly authorise an information flow based on the following rules: [**none**].

FDP_IFF.1.5(2) The TSF shall explicitly deny an information flow based on the following rules: [**none**].

6.1.4 Identification and Authentication (FIA)

6.1.4.1 FIA_ATD.1 User attribute definition

Dependences: None.

FIA_ATD.1.1 The TSF shall maintain the following list of security attributes belonging to individual users: [**identity and role**].

6.1.4.2 FIA_UAU.1 Timing of authentication

Dependences: FIA_UID.1 Timing of identification.

FIA_UAU.1.1 The TSF shall allow [**choosing the preferred language on the WebUI interface]** on behalf of the user to be performed before the user is authenticated.

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

6.1.4.3 FIA_UAU.2 User authentication before any action

Dependences: FIA_UID.1 Timing of identification.

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

6.1.4.4 *FIA_UAU.5 Multiple authentication mechanisms*

Dependencies: No dependencies.

FIA_UAU.5.1 The TSF shall provide [**username/password, VPN authentication mechanisms, MFA authentication with email/SMS code or pre-shared keys/certificates**] to support user authentication.

FIA_UAU.5.2 The TSF shall authenticate any user's claimed identity according to the [
Following rules:

- **administrators authenticate to the Console via username and password,**
- **username and password or username and email/SMS code may be used to authenticate Web users**
- **VPN can be used to authenticate remote users with multi factor authentication as option, with following options:**
    - **Username and password only**
    - **Digital certificate only**
    - **Username/password + email code**
    - **Username/password + SMS code**
    - **Username/password + digital certificate**

6.1.4.5 *FIA_UID.2 User identification before any action*

Dependences: None.

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

6.1.4.6 *FIA_AFL.1 Authentication failure handling*

Dependences: FIA_UAU.1 Timing of authentication

FIA_AFL.1.1 The TSF shall detect when [*an administrator configurable positive integer within* **[1-5]**] unsuccessful authentication attempts occur related to **[authentication attempts]**.

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been [*surpassed*], the TSF shall **[lock the account for a configurable amount of time between 30-1800 seconds]**.

6.1.4.7 *FIA_SOS.1 Verification of secrets*

Dependences: none

FIA_SOS.1.1 The TSF shall provide a mechanism to verify that secrets meet **[a password policy including:**

- **Capital letters A to Z (configurable range 0-16 for minimum requirement)**
- **Lowercase letters a to z (configurable range 0-16 for minimum requirement)**
- **Digits 0 to 9 (configurable range 0-16 for minimum requirement)**
- **Other visible characters such as semicolon, slash (configurable range 0-16 for minimum requirement)**
- **Minimum length of password (configurable range 5-16 for minimum requirement)]**.

6.1.5 Security management (FMT)

6.1.5.1 *FMT_MOF.1 Management of security functions behaviour*

Dependencies: FMT_SMR.1 Security roles
FMT_SMF.1 Specification of Management Functions

FMT_MOF.1.1 The TSF shall restrict the ability to [*determine the behaviour of, disable, enable, modify the behaviour of*] the functions [**the operations defined in table 17 for FMT_SMF.1**] to [**the authorized roles defined in table 17 for FMT_SMF.1**].

6.1.5.2 *FMT_MSA.1 Management of security attributes*

Dependencies: [FDP_ACC.1 Subset access control, or
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 [**Access Control SFP**] to restrict the ability to [*query attributes in a policy rule, delete attributes from a policy rule, add attributes to a policy rule*] the security attributes [**source zone/address, destination zone/address, service type**] to [**the authorized roles defined in table 17 for FMT_SMF.1**].

6.1.5.3 *FMT_MSA.3 Static attribute initialisation*

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

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

FMT_MSA.3.2 The TSF shall allow the [**authorized administrators according to roles defined in table 17 for FMT_SMF.1**] to specify alternative initial values to override the default values when an object or information is created.

6.1.5.4 *FMT_SMF.1 Specification of Management Functions*

Dependencies: None.

FMT_SMF.1.1 The TSF shall be capable of performing the following management functions: [**defined in table 17: Operation**].

Operation	Administrator	Administrator read-only	Auditor	Operator	User
Configure (including saving configuration)	X			X	
Configure administrator (including password reset)	X				
Update user password	X				X
Restore factory default	X				

Operation	Administrator	Administrator read-only	Auditor	Operator	User
Delete configuration file	X			X	
Roll back configuration	X			X	
Reboot	X				
View configuration information	X	X		X	
View log information	X	X	X		
Modify current admin password	X	X	X	X	

Table 17: Operation permissions for administrator roles

6.1.5.5 *FMT_SMR.1 Security roles*

Dependencies: FIA_UID.1 Timing of identification

FMT_SMR.1.1 The TSF shall maintain the roles [**defined in table 17 for FMT_SMF.1**].

FMT_SMR.1.2 The TSF shall be able to associate users with roles.

6.1.6 Protection of the TSF (FPT)

6.1.6.1 *FPT_STM.1 Reliable time stamps*

Dependencies: None.

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

6.1.7 Trusted Path/Channels (FTP)

6.1.7.1 *FTP_ITC.1 Inter-TSF trusted channel*

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 [**connections with remote: syslog servers, authentication servers, NTP server**].

6.1.7.2 *FTP_TRP.1 Trusted path*

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*].

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 [***remote administration***].

6.1.8 TOE Access (FTA)

6.1.8.1 FTA_SSL.1 TSF-initiated session locking

Dependencies: FIA_UAU.1 Timing of authentication

FTA_SSL.1.1 The TSF shall lock an interactive session after **[configurable time between 1-60 minutes for the SSH management interface, configurable time between 1-1440 minutes for the WebUI management interface]** by: a) clearing or overwriting display devices, making the current contents unreadable; b) disabling any activity of the user's data access/display devices other than unlocking the session

FTA_SSL.1.2 The TSF shall require the following events to occur prior to unlocking the session: **[new successful authentication]**.

6.2 Security Requirements Rationale

6.2.1 Relation between SFRs and security objectives

The following tracing shows which SFRs address which security objectives for the TOE.

Objectives Requirements	O.ACCESS	O.AUDIT	O.CRYPTO	O.IDAUTH	O.MANAGE	O.MEDIATE	O.PROTECT	O.REUSE	O.TIME
FAU_GEN.1		X							
FAU_GEN.2		X							
FAU_SAR.1	X	X			X				
FAU_SAR.2	X	X							
FAU_SAR.3		X			X				
FAU_STG.1		x							
FAU_STG.3		X							
FCS_CKM.1(1)			X						
FCS_CKM.1(2)			X						
FCS_CKM.4			X						
FCS_COP.1			X					X	
FCS_RNG.1			X						
FDP_ACC.1	X								
FDP_ACF.1	X								
FDP_IFC.1(1)						X			
FDP_IFC.1(2)						X			
FDP_IFF.1(1)						X			
FDP_IFF.1(2)						X			
FIA_ATD.1				X					

Objectives Requirements	O.ACCESS	O.AUDIT	O.CRYPTO	O.IDAUTH	O.MANAGE	O.MEDIATE	O.PROTECT	O.REUSE	O.TIME
FIA_UAU.2	X			X				X	
FIA_UAU.5				X					
FIA_UID.2	X			X					
FIA_AFL.1				X					
FIA_SOS.1				X					
FMT_MOF.1	X				X		X		
FMT_MSA.1	X				X		X		
FMT_MSA.3					X		X		
FMT_SMF.1					X		X		
FMT_SMR.1				X			X		
FPT_STM.1		X							X
FTP_ITC.1			X						
FTP_TRP.1			X						
FTA_SSL.1				X			X		

Table 18: Tracing of functional requirements to Objectives

The following set of justifications shows that all security objectives for the TOE are effectively addressed by the SFRs.

Security Objectives	Security Functional Requirement Rationale
O.ACCESS	The TOE must allow authorized users to access to only appropriate TOE functions and data. FAU_SAR.1 and FAU_SAR.2 ensure that only authorized administrators can access and read audit records. FDP_ACC.1 and FDP_ACF.1 ensure that only properly authorized admins can access certain functions. FIA_UID.2 and FIA_UAU.2 ensure that administrators/users are identified and authenticated prior to being allowed access to TOE security management functionality. FMT_MOF.1 ensures that only authorized administrators/users have access to security management functions. FMT_MSA.1 ensure that only authorized administrators have access to the security attributes associated with the information flow security function policies.
O.AUDIT	The TOE shall record and maintain security-related events associated with users in order to enable tracing of responsibilities for security-related acts and shall provide means to review the recorded data. FAU_GEN.1 defines the set of events that the TOE must be capable of recording. This requirement ensures that the administrator can audit any security relevant event that takes place in the TOE.

Security Objectives	Security Functional Requirement Rationale
	FAU_GEN.2 ensures that the audit records associate an administrator/user identity with the auditable event. In the case of authorized administrators/users, the association is accomplished with the user ID. In all other cases, the association is based on the source identifier, which is presumed to be the correct identity, but cannot be confirmed since these subjects are not authenticated. FAU_SAR.1 provides the means to read the audit information. FAU_SAR.2 ensures that only those specifically granted access may read the logs. FAU_SAR.3 provides a means to search the audit data. FPT_STM.1 supports the audit functionality by ensuring that the TOE can obtain a time stamp for use in recording audit events. FAU_STG.1 ensures that the TOE can protect the audit logs against unauthorized deletion. FAU_STG.3 ensures that the TOE can protect the stored audit records in case of storage exhaustion.
O.CRYPTO	The TOE must protect the confidentiality and integrity of data passed between itself and an authorized administrator, and between itself and external servers (syslog, authentication, NTP). FCS_CKM.1(1) and FCS_CKM.1(2) ensure that the TOE can generate cryptographic keys. FCS_CKM.4 provides the functionality for ensuring that keys and key material is zeroized. FCS_COP.1 requires that for each cryptographic operation an approved algorithm is used, and if compliant that the algorithm meets the standard. FTP_TRP.1 specifies the use of that cryptography between the TOE and the remote administrator. FTP_ITC.1 specifies the use of that cryptography between the TOE and the remote servers. FCS_RNG.1 supports the objective by allowing the definition of random numbers.
O.IDAUTH	The TOE must be able to identify and authenticate authorized administrators/users prior to allowing access to TOE security management functions. FIA_ATD.1 ensures that the data required to identify administrators/users is maintained by the TOE. FIA_UID.2 and FIA_UAU.2 ensure that administrators/users are identified and authenticated prior to being granted access to TOE security management functionality, and that users are identified and authenticated prior to being granted access a connected network. FIA_UAU.5 defines the available authentication mechanisms in the TOE and specifies the rules that describe how the authentication mechanisms provide authentication and when each is to be used. FMT_SMR.1 supports the objective by providing roles which are used to provide administrators/users access to TOE security functionality.

Security Objectives	Security Functional Requirement Rationale
	FIA_AFL.1 support the objective by monitoring the number of failed authentication attempts. FIA_SOS.1 supports the objective by allowing the definition of secrets complexity. FTA_SSL.1 support the objective by defining a period after which a session is locked.
O.MANAGE	The TOE must include a set of functions that allow effective management of its functions and data. The TOE will provide mechanisms to ensure that only administrators are able to log in and configure the TOE and provide protections for logged-in administrators. FAU_SAR.1 provides authorized administrators with the ability to read audit logs. FAU_SAR.3 allows authorized administrators to search audit log records. FMT_MOF.1 provides functionality to manage the behaviour of the functions/features of the TOE. FMT_MSA.1 provides the functionality to manage the parameters associated with the information flow control security functional policies. FMT_MSA.3 provides the initial values required to manage the information flow control security functional policies. FMT_SMF.1 provides the management functions supporting the specific security management claims and limiting access to that functionality to authorized administrators/users.
O.MEDIATE	The TOE must mediate the flow of all information between clients and servers located on internal and external networks governed by the TOE. FDP_IFC.1(1) and FDP_IFF.1(1) support the objective by detailing how the TOE mediates the flow of information for the unauthenticated information flow policy. FDP_IFC.1(2) and FDP_IFF.1(2) support the objective by detailing how the TOE mediates the flow of information for the authenticated information flow policy.
O.PROTECT	The TOE must protect itself and its resources from unauthorized modifications and access to its functions and data. FMT_MOF.1, FMT_MSA.1, FMT_MSA.3, FMT_SMF.1 and FMT_SMR.1 ensure that access to TOE security functions is limited to authorized administrators/users. FTA_SSL.1 ensures that sessions are locked after a defined period of time.
O.REUSE	The TOE must provide a means to prevent the reuse of authentication data for users attempting to authenticate to the TOE from a connected network. FIA_UAU.2 s requires users to be authenticated prior to access. Furthermore, FCS_COP.1 ensures that the TOE will maintain the security of the communication channels, therefore mitigating the possibility of retrieving the authentication data.
O.TIME	The TOE shall provide reliable time stamps and the capability for the administrator to set the time-source used for these time stamps, in that the administrator can configure the TOE to synchronize its clocks with NTP servers.

Security Objectives	Security Functional Requirement Rationale
	FPT_STM.1 requires that the TOE be able to provide reliable time stamps for its own use. Time stamps include date and time and are reliable in that they are always available to the TOE.

Table 19: Rationale between Objectives and SFRs

6.3 SFR Dependencies

The table below shows the dependencies of the security functional requirement of the TOE and gives a rationale for each of them if they are included or not.

SFR	Dependency	Dependency Rationale
FAU_GEN.1	FPT_STM.1	Included
FAU_GEN.2	FAU_GEN.1 FIA_UID.1	Included FIA_UID.2 is hierarchical to FIA_UID.1.
FAU_SAR.1	FAU_GEN.1	Included
FAU_SAR.2	FAU_SAR.1	Included
FAU_SAR.3	FAU_SAR.1	Included
FAU_STG.3	FAU_STG.1	Included
FCS_CKM.1(1)	[FCS_CKM.2, or FCS_COP.1] FCS_CKM.4	Included
FCS_CKM.1(2)	[FCS_CKM.2, or FCS_COP.1] FCS_CKM.4	Included
FCS_CKM.4	FDP_ITC.1, or FDP_ITC.2, or FCS_CKM.1	Included
FCS_COP.1	[FDP_ITC.1, or FDP_ITC.2, or FCS_CKM.1] FCS_CKM.4	Included
FCS_RNG.1	None	
FDP_ACC.1	FDP_ACF.1	Included
FDP_ACF.1	FDP_ACC.1 FMT_MSA.3	Included
FDP_IFC.1(1)	FDP_IFF.1	Included
FDP_IFC.1(2)	FDP_IFF.1	Included
FDP_IFF.1(1)	FDP_IFC.1 FMT_MSA.3	Included
FDP_IFF.1(2)	FDP_IFC.1 FMT_MSA.3	Included
FIA_ATD.1	None	
FIA_UAU.2	FIA_UID.1	Included FIA_UID.2 is hierarchical to FIA_UID.1.
FIA_UAU.5	None	
FIA_UID.2	None	

SFR	Dependency	Dependency Rationale
FIA_AFL.1	FIA_UAU.1	Included FIA_UAU.2 is hierarchical to FIA_UAU.1.
FIA_SOS.1	None	
FMT_MOF.1	FMT_SMR.1 FMT_SMF.1	Included
FMT_MSA.1	[FDP_ACC.1, or FDP_IFC.1] FMT_SMF.1 FMT_SMR.1	Included
FMT_MSA.3	FMT_MSA.1 FMT_SMR.1	Included
FMT_SMF.1	None	
FMT_SMR.1	FIA_UID.1	Included FIA_UID.2 is hierarchical to FIA_UID.1.
FPT_STM.1	None	
FTP_ITC.1	None	
FTP_TRP.1	None	
FTA_SSL.1	FIA_UAU.1	Included FIA_UAU.2 is hierarchical to FIA_UAU.1.

Table 20: SFR's dependencies and rationale

6.4 Security assurance requirements (SARs)

The TOE assurance requirements for this ST consist of the requirements corresponding to the EAL 4 level of assurance, as defined in the CC Part 3, augmented by the inclusion of Systematic Flaw Remediation (ALC_FLR.1). The EAL 4+ level of assurance is selected due to the following reasons:

- It represents a common CC assurance level for network related products, and in particular for firewall applications
- In includes a vulnerability assessment component (AVA_VAN.3) which is considered to represent a reasonable level for practical attacks which can be executed in the field against these types of TOEs

The assurance components are summarized in the table below.

Assurance Class	Assurance Components
ADV: Development	ADV_ARC.1 Security architecture description
	ADV_FSP.4 Complete functional specification
	ADV_IMP.1 Implementation representation of the TSF
	ADV_TDS.3 Basic modular design
AGD: Guidance documents	AGD_OPE.1 Operational user guidance
	AGD_PRE.1 Preparative procedures

Assurance Class	Assurance Components
ALC: Life-cycle support	ALC_CMC.4 Production support, acceptance procedures and automation
	ALC_CMS.4 Problem tracking CM coverage
	ALC_DEL.1 Delivery procedures
	ALC_DVS.1 Identification of security measures
	ALC_FLR.1 Basic flaw remediation
	ALC_LCD.1 Developer defined life-cycle model
	ALC_TAT.1 Well-defined development tools
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
	ASE_TSS.1 TOE summary specification
ATE: Tests	ATE_COV.2 Analysis of coverage
	ATE_DPT.1 Testing: basic design
	ATE_FUN.1 Functional testing
	ATE_IND.2 Independent testing - sample
AVA: Vulnerability assessment	AVA_VAN.3 Focused vulnerability analysis

Table 21: Assurance requirements

7 TOE Summary Specification

7.1 TOE Security Functions Specification

This section describes the security functions provided by the TOE to meet the security functional requirements specified for the TOE in section 6.1 Security Functional Requirements (SFRs).

The table below shows the mapping between the SFRs, and the implementing security functions, and a description is given in the following subsections.

Objectives Requirements	SF.ACCESS	SF.AUDIT	SF.AUTHENTICATION	SF.COMMUNICATION	SF.CRYPTOGRAPHY	SF.MANAGEMENT
FAU_GEN.1		X				
FAU_GEN.2		X				
FAU_SAR.1		X				
FAU_SAR.2		X				
FAU_SAR.3		X				
FAU_STG.1		x				
FAU_STG.3		X				
FCS_CKM.1(1)					X	
FCS_CKM.1(2)					X	
FCS_CKM.4					X	
FCS_COP.1					X	
FCS_RNG.1					X	
FDP_ACC.1	X					
FDP_ACF.1	X					
FDP_IFC.1(1)				X		
FDP_IFC.1(2)				X		
FDP_IFF.1(1)				X		
FDP_IFF.1(2)				X		
FIA_ATD.1			X			
FIA_UAU.2			X			
FIA_UAU.5			X			
FIA_UID.2			X			
FIA_AFL.1			X			
FIA_SOS.1			X			
FMT_MOF.1	X					X
FMT_MSA.1						X
FMT_MSA.3				X		X
FMT_SMF.1						X
FMT_SMR.1	X					X
FPT_STM.1		X				
FTP_ITC.1					X	
FTP_TRP.1					X	
FTA_SSL.1	X					

Table 22: Mapping SFRs to security functions

7.1.1 SF.ACCESS

(FDP_ACC.1, FDP_ACF.1, FMT_MOF.1, FMT_SMR.1)

The TOE can manage administrator access and interaction with TOE data. The TOE enforces access control policy based on security attributes of users, which limits access to the TOE data and to the TOE configuration settings. Access to TOE data and settings is enforced by administrator account privileges (permissions). A user attempting to access the TOE with the incorrect privileges will be denied access.

Only authorized administrator accounts can login to TOE, through a secure local CLI interface or by means of a network Web-based GUI supported by an AAA server. The TOE has four roles for the administration, which are Administrator, Administrator read-only, Auditor, and Operator. Once granted access to the TOE, the administrators with the correct privileges can manage TOE data.

(FTA_SSL.1)

The TOE can control the open sessions for the administrator and lock an interactive session after a defined period of time, which is configurable for both the SSH, as well as the WebUI interfaces.

7.1.2 SF. AUDIT

(FAU_GEN.1, FAU_GEN.2)

The TOE generates a comprehensive set of audit logs that identify specific TOE operations whenever an auditable event occurs, for administrative events, potential policy violations and information flow decisions:

- Device log
  - Event - includes 8 severity levels: debugging, information, notification, warning, error, critical, alert, and emergency.
  - Network - logs about network services, like PPPoE and DDNS.
  - Configuration - logs about configuration on command line interface, e.g. interface IP address setting.
- Share Access Logs - logs about share access rule.
- Threat - logs related to behaviors threatening the protected system, e.g. attack defense and application security.
- Session - Session logs, e.g. session protocols, source and destination IP addresses and ports.
- NAT - NAT logs, including NAT type, source and destination IP addresses and ports.
- EPP - logs related with end point protection function.
- File Filter - logs related with file filter function.
- Content filter logs – logs related with content filter function, e.g. Web content filter, Web posting, Email filter and
- HTTP/FTP control.
- Network behavior record logs – Logs related with network behavior record function, e.g. IM behavior.
- URL - logs about network surfing, e.g. Internet visiting time, web pages visiting history, and URL filtering logs.
- PBR - logs about policy-based route.

The logging feature records various kinds of system logs, including device log, threat log, session log, NAT log, Content filter log, File filter log, Network Behavior Record logshare access logs, and URL logs.

The logs have descriptions that indicate the following information:

- The date and time the action was initiated.

- The severity level according to the defined types of events (Emergencies, Alerts, Critical, Errors, Warnings, Notifications, Informational, Debugging).
- The identity of the subject that caused the event.
- The outcome of the event.

(FAU_SAR.1, FAU_SAR.2, FAU_SAR.3)
The authorized administrators can read the audit records, according to the role privileges. Log messages can be sent to the following destinations:

- Console - The default output destination.
- Remote - Includes SSH.
- Buffer - Memory buffer.
- File - By default, the logs are sent to the specified USB destination in form of a file.
- Syslog Server - Sends logs to UNIX or Windows Syslog Server.
- Email - Sends logs to a specified email account.
- Local database - Sends logs to the local database of the device.

(FPT_STM.1)
The TOE provides a source of date and time information used in audit event timestamps, receiving clock updates from an NTP server (IPv6 supporting).

(FAU_STG.1, FAU_STG.3)
The TOE provides a mechanism to protect the stored logs against deletion, and against storage exhaustion. The TOE implements this by detecting a certain storage threshold of audit being reached, and offering a configurable option, including stopping the log action, or overriding the early audit events.

7.1.3 SF. AUTHENTICATION

(FIA_ATD.1, FIA_UAU.2, FIA_UAU.5, FIA_UID.2)

In the TOE, authentication supports the following five types of AAA server:

- Local server: a local server is the firewall itself. The firewall stores user identity information and handles requests, but its storage space is limited by the firewall hardware size.
- External servers:
  - Radius Server (supporting IPv6).
  - TACACS+ Server.
  - LDAP Server.
  - Active-Directory (AD) Server.

The TOE can identify administrators by a unique ID and enforces their authentication before granting them access to any TSF management interfaces. Detailed functions include support for:

- Local CLI interface, by means of Console or SSH.
- WebUI, by means of HTTPS (IPv6 supporting).

This authentication is supported either by a Local Server, Radius Server, TACACS+ Server, LDAP Server, or AD Server.

Users can access to network through the TOE with or without authentication, depending on the configuration on the TOE. If the administrator has setup authentication force for TOE users, a user can be authenticated through:

- Web Authentication, or VPN.

This authentication is supported either by a Local Server, Radius Server, TACACS+ Server, LDAP Server, or AD Server.

When a security product enables authentication, the users and hosts can be denied or allowed to access certain networks. From a user's point of view, authentication is divided into the following categories:

- A user from an internal network who wants to access the Internet can use:
    - Web Authentication: After the Web authentication is configured, and a browser is opened to access the Internet, the page will redirect to the WebAuth login page.
- A user from the Internet who wants to visit an internal network can use:
    - SSL VPN: The TOE device provides an SSL based remote access solution. Remote users can access the Intranet resource safely through the provided SSL VPN.
    - IPsec VPN: IPsec protocol defines how to choose the security protocols and algorithms, as well as the method for exchanging security keys among communicating peers.

(FIA_AFL.1)

The TOE provides a mechanism to detect when a number of incorrect authentication attempts has been reached for the administrator interface. The number of incorrect attempts is configurable.

(FIA_SOS.1)

The TOE allows for the verification that secrets meet a certain minimum set of criteria, based on a configurable password complexity policy.

7.1.4 SF.COMMUNICATION

(FDP_IFC.1(1), FDP_IFC.1(2), FDP_IFF.1(1), FDP_IFF.1(2), FMT_MSA.3)

The TOE operates in accordance with two information flow security functional policies:

- The Unauthenticated Information Flow SFP allows unauthenticated users to pass information through the TOE, with firewall mediation according to the firewall rules defined by an authorized administrator.
- The Authenticated Information Flow SFP allows authenticated users to pass information through the TOE, with firewall mediation according to the firewall rules defined by an authorized administrator.

Security policy is the basic function of devices that is designed to control the traffic forwarding between security zones/segments. Without security policy rules, the devices will deny all traffic between security zones/segments by default. After configuring the security policy rule, the device can identify what traffic between security zones or segments will be permitted, and the others will be denied.

The basic elements of policy rules:

- The source zone and address of the traffic.
- The destination zone and address of the traffic.
- The service type of the traffic.
- Actions that the devices will perform when processing the specific type of traffic, including Permit, Deny, Tunnel, From tunnel, WebAuth, and Portal server.

Regardless of firewall rules, packets which include parameters as specified by the security functional requirements which define the security functional policies are never permitted to pass through the TOE. Modification of the rules is restricted to an authorized administrator, and an authorized administrator may also specify alternative initial values to override the default values. The TOE allows an authorized administrator to view all information flows allowed by the information flow policy rules before the rules are applied.

Generally, a security policy rule consists of two parts: filtering conditions and actions. The administrator can set the filtering conditions by specifying traffic's source zone/address, destination zone/address, service type, and user. Each policy rule is labeled with a unique ID which is automatically generated when the rule is created. The administrator can also specify a policy rule ID at own choice. All policy rules in system are arranged in a specific order. When traffic flows into a device, the device will query for policy rules by turn, and processes the traffic according to the first matched rule.

The max global security policy rule numbers may vary in different models.

Security policy supports IPv4 and IPv6 address. If IPv6 is enabled, the administrator can configure IPv6 address entry for the policy rule.

7.1.5 SF.CRYPTOGRAPHY

(FCS_CKM.1(1), FCS_CKM.1(2))

In support of secure cryptographic protocols, the TOE supports the key generation schemes of RSA and DSA as specified in FIPS PUB 186-4, and of 3DES and AES as specified in NIST SP 800-135 Revision 1.

(FCS_CKM.4)

The TOE meets all requirements specified in FIPS 140-2 for destruction of keys. All these keys within the TOE are zeroizable.

(FCS_COP.1)

The TOE provides Encryption and Decryption capabilities:

- Using 192 bits 3DES, described in NIST SP 800-67.
- Using 128, 192, and 256 bits AES, described in FIPS PUB 197.

The TOE provides Key Exchange capabilities:

- Using 2048, 3072, and 4096 bits Diffie-Hellmann.

The TOE provides Hashing capabilities:

- Using 128 bits MD5.
- Using 160, 256, 384, and 512 SHA, described in FIPS PUB 180-4.

The TOE provides HMAC capabilities:

- Using 128 bits MD5.
- Using 160, 256, 384, and 512 SHA, described in FIPS PUB 198-1.

The TOE provides Digital Signature capabilities:

- Using 2048 bits RSA and DSA, described in FIPS PUB 186-4.

(FTP_TRP.1)
The TOE contains functionality for PKI, which is used in the following two situations:

- PKI can be used by IKE VPN tunnel.
- PKI applies to the situation where a user accesses the TOE over HTTPS or SSH.

The TOE provides trusted paths and trusted channels, protected by encryption to guard against disclosure and protected by cryptographic signature to detect modifications. The trusted paths and trusted channels are logically distinct from other communication paths and provide assured identification of their end points.

The trusted paths are used to protect remote administrator authentication, all remote administrator actions, Proxy user authentication, VPN user authentication, and all VPN user actions. Remote administration sessions apply to the Network Web-Based GUI.

(FTP_ITC.1)
The TOE uses IPsec, SSH, and TLS to protect communications between itself and remote entities for the following purposes:

- The TOE protects transmission of audit records when sending syslog message to a remote audit server by transmitting the message over SSL/TLS (OpenSSL library v1.1.1) or IPsec.
- Connections to authentication servers (AAA servers) can be protected via IPsec tunnels. Connections with AAA servers (via RADIUS and TACACS+) can be configured for authentication of TOE administrators.
- SSH sessions can be initiated from the TOE to remote SSH servers, such as other network devices, for the purposes of remotely administering remote devices.
- Connections to NTP servers can be protected via IPsec tunnels.

(FCS_RNG.1)
The TOE generates random numbers to be further used in crypto operations such as key generation, SSL/TLS negotiation, IKE negociation.

7.1.6 SF.MANAGEMENT

(FMT_MOF.1, FMT_MSA.1, FMT_MSA.3, FMT_SMF.1, FMT_SMR.1)

Appropriately authorized administrators may configure TOE data (including saving configuration), configure administrator, restore factory default, delete configuration file, roll back configuration, reboot StoneOS, view configuration information, view log information, modify current admin password, and perform ping and traceroute tests. The Netconf protocol is supported for management actions.

The TOE ensures that only authorized users can specify the policy definitions to enforce availability. By default, the TOE provides a permissive information flow policy rule set.

The TOE provides all the capabilities necessary to securely manage the TOE. The authorized administrator can connect to the TOE either via CLI or through the TOE GUI to perform these functions. All general administration is expected to take place through the Web UI.

The TOE authenticates all access to the administrative and management interfaces using a username and password. The TOE supports local administration through the CLI and management through Web UI, by means of the roles: Administrator, Administrator read-only, Auditor, and Operator.