McAfee NGFW and McAfee NGFW-IPS 5.5 Security Target

VERSION 2.0

2014-05-27

McAfee, Inc. (An Intel Company)
2821 Mission College Blvd.
Santa Clara, CA 95054
USA

TABLE OF CONTENTS

List of Figures and Tables

Document History

Version	Date	Authors	Comment
1.0pre1	2013-05-29	Staffan Persson, atsec	First draft version based on the StoneGate Firewall Security Target
1.0pre2	2013-06-11	Staffan Persson, atsec	An update with more complete information on the VPN and IDS aspects
1.0pre3	2013-06-17	Staffan Persson, atsec	Updated the description of IPS functionality with major input from Stonesoft
1.0pre4	2013-07-03	Staffan Persson, atsec	Fixed some typos and updated the description of the FCS components.
1.0pre5	2013-08-09	Staffan Persson, atsec	Fixed after Stonesoft and evaluator comments.
1.0pre6	2013-08-26	Staffan Persson, atsec	Minor fixes to the extended components.
1.0	2013-09-02	Staffan Persson, atsec	Fixed after evaluator comments.
1.1	2013-10-24	Staffan Persson, atsec	Fixed after certifier comments and updates from Stonesoft
1.2	2013-10-29	Staffan Persson, atsec	Fixed the IPS rule-set based due to comments from Stonesoft
1.3	2013-11-05	Staffan Persson, atsec	Clarified some SFRs for FCS and FDP.
1.4	2013-11-11	Staffan Persson, atsec	Updated some SFRs for FCS and cipher suites being used
1.5	2013-12-11	Jorma Levomäki and Staffan Persson	Updated the FCS SRFs and dependencies
1.6	2013-12-18	Jorma Levomäki and Staffan Persson	Updated due to evaluator comments
1.7	2014-02-19	Jorma Levomäki and Staffan Persson	Updated due to evaluator comments
1.8	2014-03-20	Jorma Levomäki and Staffan Persson	Updated title and developer name
1.9	2014-05-02	Jorma Levomäki	Updated TOE identification
2.0	2014-05-27	Jorma Levomäki	Updated the guidance references

1 INTRODUCTION

1.1 SECURITY TARGET IDENTIFICATION

Title:	McAfee NGFW and McAfee NGFW-IPS 5.5 Security Target
Version	2.0
Status:	Released
Date:	2014-05-27
Sponsor:	McAfee, Inc. (An Intel Company)
Developer	McAfee, Inc. (An Intel Company)
Keywords:	Firewall, VPN, IPS, Intrusion Detection and Prevention, High Availability, Traffic Filter, Application Proxy

1.2 TOE IDENTIFICATION

Stonesoft Firewall/VPN & IPS Security Engine, version 5.5.4.9869.cc.2

1.3 TOE OVERVIEW

1.3.1 TOE Type

The TOE, the Stonesoft Firewall/VPN & IPS Security Engine, is a network protection software component running on an appliance. It may be operated either as a Layer 3 Firewall with VPN or as a transparent Layer 2 Intrusion Prevention System (IPS).

Operated as Firewall/VPN it provides a Multi-Layer Inspection technology that combines both stateful and application-level inspection technology to control connectivity and information flow between internal and external networks. It also provides a means to keep the internal hosts' IP-address private from external users. As part of a cluster, the Stonesoft Firewall/VPN & IPS Security Engine provides high availability of these firewall security services for the users and servers protected by the cluster of firewalls when a node in the cluster or a network connection to a node fails.

Operated as IPS, it provides Multi-Layer Inspection technology combined with evasion-proof threat protection and flexibility in network deployment.

1.3.2 Required Hardware and Software

The Stonesoft Firewall/VPN & IPS Security Engine is able to run on either a Stonesoft appliance, on an Intel x86 based server or compatible hardware, or as a virtual appliance on a VMware hypervisor. However, in the evaluated configuration the TOE is provided and running as part of a Stonesoft appliance with hardware and underlying operating system consisting of

- a standard Intel Pentium 4 or higher based hardware platform with 2 GB or more RAM with four or more network interfaces, and
- a Debian GNU/Linux 6.0 based operating system including a Linux kernel 3.5.7 with Stonesoft specific modifications.

Please see chapter 1.4.2.1 for the specific hardware models that are part of the evaluated configurations. A detailed list of hardware and software components that are considered part of the TOE environment is provided in chapter 1.4.2.5.

For the operation and management of the Stonesoft Firewall/VPN & IPS Security Engine a separate management client and server is needed. The server will be running the Stonesoft Management Center (SMC), which is a Java-based management system. A log server is also needed, as well as an authentication server. All of these clients and servers are part of the TOE environment.

1.3.3 Intended Method of Use

The Stonesoft Firewall/VPN & IPS Appliance product in Firewall/VPN role is intended to be used as a network perimeter security gateway that provides a controlled connection. It may be used part of a cluster or as the sole connection between an internal network and an external, untrusted network.

The Stonesoft Firewall/VPN & IPS Appliance product in IPS role is intended to be used for network traffic deep inspection and threat protection. The intended IPS deployment scenarios are (but not limited to) network perimeter, network core and internal network segments.

The Stonesoft Firewall/VPN & IPS Appliance is assumed to be installed and operated within a physically protected environment, administered by trusted and trained administrators over a trusted and separate management network.

In the evaluated configuration, the Stonesoft Firewall/VPN & IPS Security Engine may be operated in one of two roles (modes of operation), each providing a different set of security functionality. The Stonesoft Firewall/VPN & IPS Security Engine may be used either as a Firewall/VPN or as an IPS. Multiple installations of the Stonesoft Firewall/VPN & IPS Security Engine may be used in combination to obtain the functionality of both the Firewall/VPN or the IPS role.

The Stonesoft Firewall/VPN & IPS Security Engine runs on a hardened Linux operating system that is shipped with the product. The software runs on a single or multi-processor Intel platform, which is also part of the Stonesoft Firewall/VPN & IPS Appliance product.

A distributed management system comprising a Management Server, Log Server and Graphical User Interface (GUI) to support the management and operation of the firewall is supplied as a separate product.

1.3.4 Major Security Features

The TOE can be operated in two different, distinct roles: the Firewall/VPN role and the IPS role. Depending on the role, the TOE provides a different set of security functionalities:

Operated in the Firewall/VPN role it provides information flow control using multi-layer inspection (layer 3) including packet filtering, virtual private network connections (VPN) authenticating and encrypting data traffic to remote nodes over untrusted networks.

Operated in the IPS role it provides intrusion detection and prevention (IDS/IPS) using a range of different intrusion detection mechanisms including protocol decoding and normalization on all protocol layers. Connection state, protocol specific inspection modules and file contexts provide accurate signature matching context in the normalized data stream.

Independent of the role, the Stonesoft Firewall/VPN & IPS Security Engine is centrally managed and generates audit records for security critical events.

The Stonesoft Firewall/VPN & IPS Security Engine can also be updated using the update mechanisms both for the engine as well as for the fingerprints used by the IPS. This mechanism is not part of the evaluated configuration.

1.4 TOE DESCRIPTION

1.4.1 Introduction

The Stonesoft Firewall/VPN & IPS Security Engine is a high availability network protection appliance for securing data communications and enabling continuous network connectivity. The TOE may be operated either as a Firewall/VPN or as an Intrusion Prevention System (IPS).

The TOE is intended for use by organizations, which need controlled, protected and audited access to services, both from inside and outside their organization's network. The TOE provides mechanisms for encrypting, allowing, denying, analyzing and/or redirecting the flow of data through the TOE.

The TOE is the Stonesoft Firewall/VPN & IPS Security Engine, which is a software component of the Stonesoft Firewall/VPN & IPS Appliance product. The Stonesoft Firewall/VPN & IPS Appliance comprises the security engine; the OpenSSL, OpenSSH and OpenLDAP components; the operating and the hardware. The scope of the TOE is the security engine only. Other components of the appliance as well as the management client, management server and log server are outside of the scope of the evaluation.

To support the operations of the security engine, the separately supplied management system includes a Management Server that provides a trusted interface for administrator functions, a Log Server to store and manage (i.e., filter, sort, archive) the log records, and a GUI to facilitate administrator access. Its distributed architecture makes it flexible and scalable since it can run on single or on multiple hardware platforms. The Management Server provides support for the following operating systems: Microsoft Windows Server 2008 SP2 and R2, Windows 7 SP1, Windows Vista SP2, Windows Server 2003 SP2 (32-bit), CentOS 6, Red Hat Enterprise Linux 6 and SUSE Linux Enterprise 11 SP1.

The Security Engine uses a hardened Linux operating system based on Debian GNU/Linux. All non-essential packages have been removed from the Debian distribution.

The Stonesoft Firewall/VPN & IPS Security Engine can operate as a node or as part of a cluster consisting of 2-16 nodes, illustrated as **FW**^{ooo} in Figure 1, Stonesoft Security Platform shown below. The cluster is required for high availability of security services. Each node has internal and external network connections for which it provides its security services. In the case the Stonesoft Firewall/VPN & IPS Security Engine is operated in IPS role, there is no clustering so the term node refers to the local IPS.

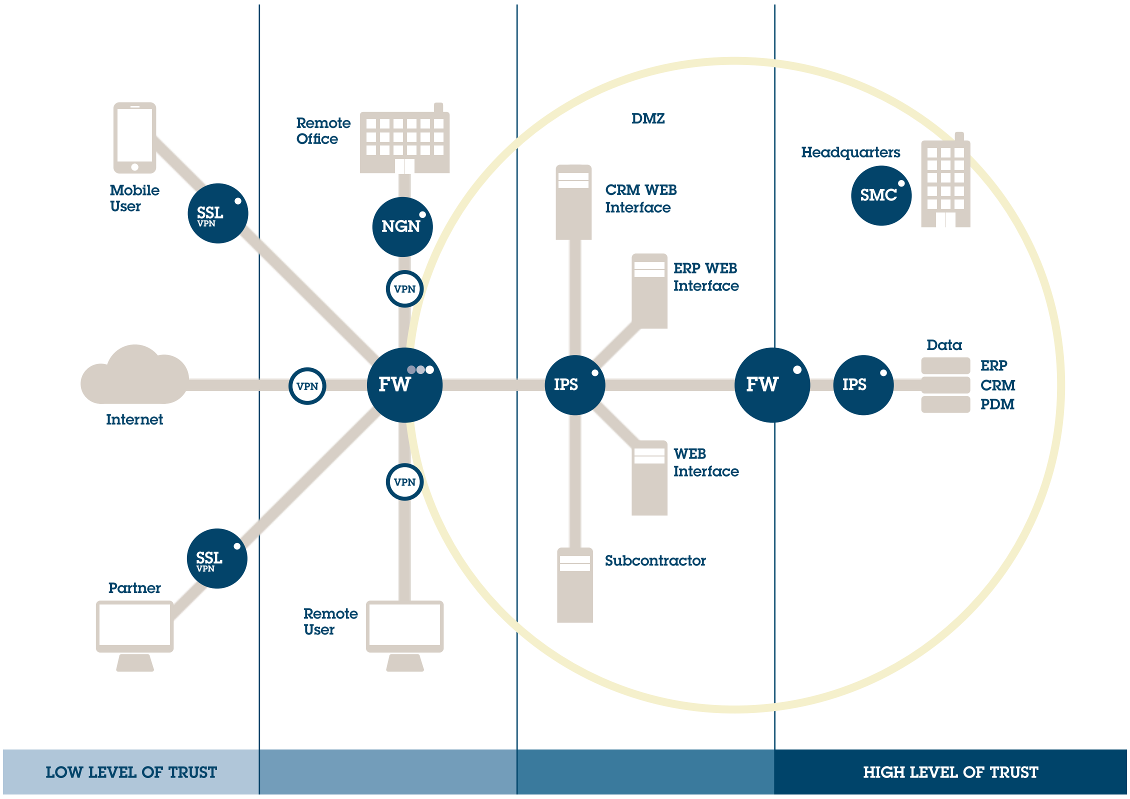

Figure 1, Stonesoft Security Platform

The nodes can have separate management networks for connectivity to the management system and the other nodes in a cluster, i.e., management network and cluster network, respectively. This is also the environment for the evaluated configuration.

The IT environment of the Stonesoft Firewall/VPN & IPS Appliance comprises the Stonesoft Management Center (SMC) (shown as Management Client, Management Server and Log Server in the Figure 2 below).

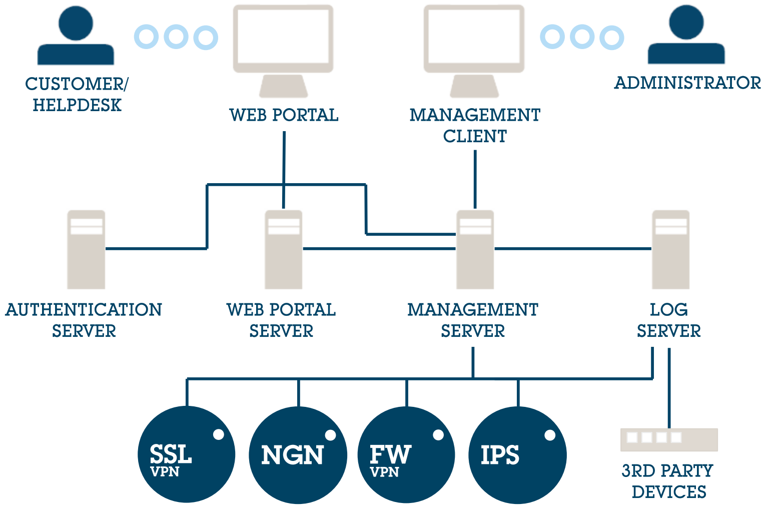

Figure 2, Stonesoft Architecture

1.4.2 **TOE Scope**

1.4.2.1 Hardware Platforms

The following Stonesoft Firewall/VPN & IPS Security Engine appliance models are included within the evaluation scope:

- Stonesoft MIL-320 (Firewall/VPN only)
- Stonesoft 5206
- Stonesoft 3206
- Stonesoft 3202
- Stonesoft 1402
- Stonesoft 1065
- Stonesoft 1035

1.4.2.2 Physical

The physical scope of the TOE is illustrated in Figure 3 below.

It comprises the Security Engine software application, version 5.5.4.9869.cc.2, including:

- the Firewall component
- the IPS component
- the INSIDE Secure QuickSec IPsec Toolkit, version 5.2 (the VPN component)

running on one of the platforms listed in chapter 1.4.2.1.

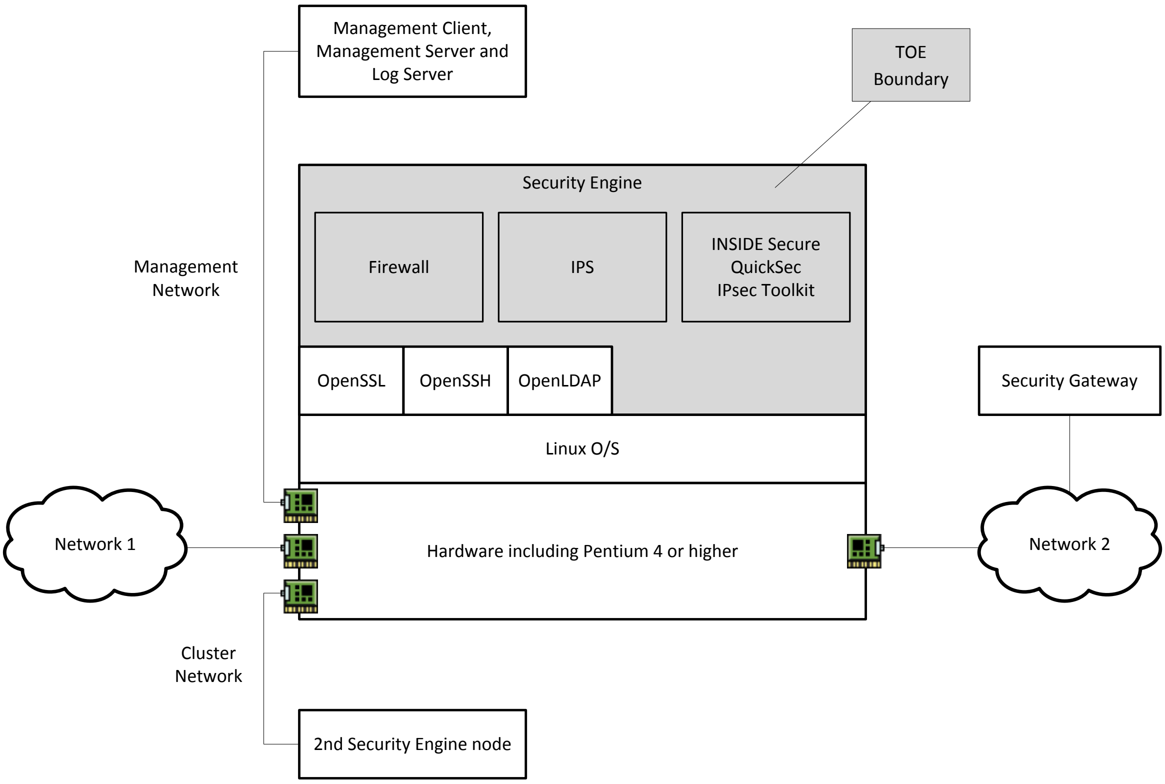

Figure 3 TOE Boundary and IT Environment

The documentation is included with the scope of the TOE and consists of the following guides:

- Stonesoft Firewall/VPN Installation Guide [1]
- Stonesoft Firewall/VPN Reference Guide [2]
- Stonesoft IPS and Layer 2 Firewall Installation Guide [3]
- Stonesoft IPS and Layer 2 Firewall Reference Guide [4]
- Stonesoft Administrator’s Guide [5]

- Common Criteria Certification User's Guide [6]

The documentation is available for download from the Stonesoft website.

1.4.2.3 Logical

In this ST there are two different roles (modes) for using the Stonesoft Firewall/VPN & IPS Security Engine, the Firewall/VPN and the IPS roles. Depending on the role different security functionality will be available. The security features within the scope of the ST when operated in the Firewall/VPN role are:

- Information Flow Control on the traffic that passes through the TOE. The TOE mediates the flow of all information that passes through its internal and external network connections to enforce the firewall security policy using:
    - Access rules based on the IP source address, destination address, transport layer protocol, application layer protocol, source port, destination port, and the interface on which the packet arrives; connection tracking; user authentication results; and the validity time.
    - Protocol Agents providing additional rules based on application-level information and mechanisms to redirect connections. The evaluation is limited to protocol agents for FTP, HTTP, and SMTP. All other protocol agents are not part of the evaluated configuration.
- Network Address Translation (NAT) between external IT entities that pass traffic through the TOE, ensuring that the IP addresses of hosts on internal networks are kept private from external users.
- Virtual Private Network: IPsec compliant VPN (tunnel mode only) using IKE for key establishment with certificate based authentication. SSL-based VPN connections are not included in the evaluated configuration.
- High Availability: In case of a total node failure, failure in one component or loss of connectivity to a network connected to a node, the firewall engine in a cluster is capable of failing over all sessions to other nodes. This provides continuous enforcement of the firewall security policy, including information flow control.

The security features within the scope of the ST when operated in the IPS role are:

- Deep packet inspection for the following protocols: Ethernet, IPv4, TCP, UDP, DNS, and HTTP
- Context-aware inspection, in which the inspection is protocol specific
- Fingerprinting

Both the Firewall/VPN and the IPS provides the following major security features:

- Audit generation: The TOE provides a means to generate audit records of security-relevant events relating to the IP traffic through the firewall and firewall security policy changes. The TOE also provides a means for the administrator to define the criteria used for the selection of the IP traffic events to be audited. It also provides a mechanism for preventing audit data loss.
- Security manageability and protection of security functions: Administrators access the TOE using certificate based authentication and protected communication between the Stonesoft Management Center (not part of the TOE) and TOE. The Stonesoft Management Center provides the interface for managing the security policy and authentication attributes, the TSF data, and security functions of the TOE. The TOE also ensures the trusted security functions are always invoked and cannot be bypassed.

1.4.2.4 Configurations

The evaluated configuration of the TOE specifies:

- Connection tracking enabled;
- Log spooling policy set to 'stop traffic';
- Access to the command line interface to the Security Engine from the operating system is disabled as specified in the installation documentation;

1.4.2.5 TOE Environment

The operational environment for the evaluated configuration includes one of the appliances listed in section 1.4.2.1 satisfying the requirements below. TOE operating platform and the software running on it are delivered with the TOE. The Stonesoft Management Center must be acquired separately.

- TOE operating platform:

  - Intel Pentium 4 or higher (or equivalent) recommended,
  - 2 GB RAM or more recommended,
- Standard Linux Kernel 3.5.7 with Stonesoft specific modifications, Debian GNU/Linux 6.0 (squeeze) based distribution,
  - Network Interface Cards (see Annex D).
- Stonesoft Management Center, version 5.5:
  - the Management Server,
  - the Log Server,
  - the Management Client,
- OpenSSL 1.0.1 and 0.9.8,
- OpenSSH 5.5,
- OpenLDAP client and server, version 2.4,
- Architecture and System support:
  - at least 2 network interfaces,
  - 1 management network interface,
  - 1 cluster network interface (applicable only for Firewall/VPN),
  - a second TOE to form a cluster (applicable only for Firewall/VPN), and
  - a third TOE used as a Security Gateway for VPN functionality (applicable only for Firewall/VPN).

2 CONFORMANCE CLAIM

This TOE conforms to the following CC specifications:

- Common Criteria for Information Technology Security Evaluation Part 2: Security functional requirements, Version 3.1, Revision 4, September 2012. CC Part 2 extended.

  The extended component FAU_STG.NIAP-0414 is used to express additional functionality contained within NIAP interpretation 0414. The extended components FCS_IPSEC_EXT.1 and FCS_RBG_EXT are used to express requirements for the IPsec VPN.

- Common Criteria for Information Technology Security Evaluation Part 3: Security assurance requirements, Version 3.1, Revision 4 September 2012. CC Part 3 conformant.

The assurance package conformance is Evaluation Assurance level 4 (EAL4) augmented with ALC_FLR.1, Basic flaw remediation. No Protection Profile conformance is claimed.

3 SECURITY PROBLEM DEFINITION

The security problem definition defines the security problem that is addressed by the TOE as well as the assumptions on the operational environment that are necessary for the TOE to be able to address the security problem. Since the TOE can operate either in the role of Firewall/VPN or in the role of IPS any assumption, threat or organizational security policy only applicable to a certain role are marked with {Firewall/VPN} or {IPS} and the ones applicable for both roles are not marked.

3.1 ASSUMPTIONS

This section of the security problem definition describes the assumptions that must be satisfied by the operational environment of the TOE.

A.ADMIN	It is assumed that the administrator only can access the TOE via the trusted Management Server on a trusted and separate management network and that the administrator has been identified and authenticated to the Stonesoft Management Center.
A.ADMINTRUST	It is assumed that administrators are trained, qualified, non-hostile and follow all guidance.
A.AUDITMAN	It is assumed that audit trails are regularly analyzed and archived.
A.AUDITSUPP	It is assumed that the environment provides protected permanent storage of the audit trails generated by the TOE.
A.MEDIATSUPP	It is assumed that data cannot flow between the internal and external networks unless it passes through the TOE. In the cluster case (Firewall/VPN role only), traffic only needs to pass through one of the cluster nodes, which is just another instance of the TOE.
A.ENVIRON	It is assumed that the underlying hardware of the TOE node and the TOE's associated Management Servers and management and cluster networks are dedicated to the TOE usage, function according to their specifications, and are physically secure, only allowing administrators physical access.
A.TIME	It is assumed that the IT environment will provide a reliable time source to the TOE and the TOE environment.
A.USERAUTH {Firewall/VPN}	It is assumed that the IT environment will provide a user directory and a user authentication mechanism for the TOE to use when the firewall security policy requires users to authenticate before information can flow between the internal and external networks.
A.VPN {Firewall/VPN}	Peer external IT entities in trusted VPN channels must be able to protect the integrity and confidentiality of data transmitted to the TOE via encryption and provide authentication for such data. Upon receipt of data from the TOE, the peer external IT entity must be able to decrypt the data and verify that the received data accurately represents the data that was originally transmitted.
A.PLACEMENT {IPS}	The IPS must be placed in such a way to ensure adequate coverage of network segments where critical assets are located.

3.2 THREAT ENVIRONMENT

This section of the security problem definition describes the threats that are countered by the TOE, its operational environment, or a combination of the two.

The assets to be protected are:

- External access to user data and IT resources within the network perimeter of the TOE;
- User data that is transmitted over the VPN channel provided by the TOE in the VPN role;
- The TSF and TSF data, including the configuration data and the audit data.

The threat agents are either external unauthorized persons or external IT entities not authorized to use the TOE itself.

T.UNDETECTED	**Security Events Go Undetected** A threat agent may attempt to compromise the assets without being detected. This threat includes a threat agent causing audit records to be lost or prevent future records from being recorded by taking actions to exhaust audit storage capacity, thus masking an attacker's actions.
T.MEDIAT	**Information Flow Control** A threat agent may send information through the TOE, which results in the exploitation and/or compromise of IT assets. This threat includes unauthorized entities attempting to bypass the information flow control policy by sending an IP packet with a fake source address.
T.ACCESS	**Unauthorized access** A threat agent may access TOE management functions and read, modify, or destroy security critical TSF data or tampering with the TSFs.
T. FAILURE {Firewall/VPN}	**Denial of Service Prevention** A failure of a node or a network connection to a node caused by a threat agent or due to the failure of TOE components could cause denial of service, making assets unavailable.
T.DISCLOSE {Firewall/VPN}	**Disclosure of Information Transmitted** A threat agent in the external network gains unauthorized access to data transmitted between the TOE and a remote trusted network.
T.MODIFY {Firewall/VPN}	**Modification of information Transmitted** Failure to detect modifications made by a threat agent located in the external network of data transmitted between the TOE and a remote trusted network.

3.3 ORGANISATIONAL SECURITY POLICIES

This ST defines the following organizational security policies to be addressed by the TOE and its operational environment.

P.MANAGE	The TOE shall support the means to be managed by administrators to configure and manage the TSFs.
P.HIDE {Firewall/VPN}	The TOE must provide a means to hide the IP addresses of hosts on the internal network and of network topology of the internal network.
P.INSPECT {IPS}	The TOE shall perform inspection of the information flowing through the TOE and ensure that any information flow allowed through is consistent with the applicable information flow control policies.

4 SECURITY OBJECTIVES

4.1 SECURITY OBJECTIVES FOR THE TOE

O.AUDIT	The TOE must provide a means to accurately detect and record security-relevant events in audit records, and prevent audit data loss by prioritizing and preventing security-relevant events when the audit storage capacity fills.
O.MANAGE	The TOE must provide a means for an administrator via the Management Server to manage the TOE security functions.
O.MEDIAT	The TOE must mediate the flow of all information between users and external IT entities on the internal and external networks connected to the TOE in accordance with its security policy.
O.AVAILABILITY {Firewall/VPN}	The TOE when operating as part of a firewall cluster must provide high availability of information flow control, ensuring continuation of service when firewall nodes or their interfaces fail.
O.HIDE {Firewall/VPN}	The TOE must provide a means to hide the IP addresses of hosts on the internal network and of the network topology of the internal network.
O.CHANNEL {Firewall/VPN}	The TOE must be able to provide trusted channels to remote trusted networks and protect information transmitted to and received from such networks against unauthorized disclosure and to detect any modification of incoming information transmitted from such networks, and to provide the means for the remote network to verify the integrity of information transmitted out of the TOE to such networks.
O.INSPECT {IPS}	The TOE shall perform inspection of the information flowing through the TOE and ensure that any information flow allowed through is consistent with the applicable information flow control policies.

4.2 SECURITY OBJECTIVES FOR THE ENVIRONMENT

OE.ADMIN	The environment has to ensure that the administrator only accesses the TOE via the trusted Management Server on a trusted and separate management network and that the administrator has been identified and authenticated to the Stonesoft Management Center.
OE.ADMINTRUST	The environment has to ensure that administrators are trained, qualified, non-hostile and follow all guidance.
OE.AUDITMAN	The environment has to ensure that audit trails are regularly analyzed and that they are archived.
OE.AUDITSUPP	The environment has to ensure that it provides protected permanent storage of the audit trails generated by the TOE.
OE.MEDIATSUPP	The environment has to ensure that the TOE is the only connection between internal and external networks. In the cluster case (Firewall/VPN role only), the information flow only needs to pass through one of the cluster nodes, which is just another instance of the TOE.
OE.ENVIRON	The environment has to ensure that the underlying hardware of the TOE node and the TOE's associated Management Servers and management and cluster networks are dedicated to the TOE usage, function according to their specifications, and are physically secure, only allowing administrators physical access.
OE.TIME	The IT environment has to provide a reliable time source to the TOE and the TOE environment.
OE.USERAUTH {Firewall/VPN}	The IT environment has to provide a user directory and a user authentication mechanism for the TOE to use when the firewall security

	policy requires users to authenticate before information can flow between the internal and external networks.
OE.VPN {Firewall/VPN}	Peer external IT entities in trusted VPN channels must be able to protect the integrity and confidentiality of data transmitted to the TOE via encryption and provide authentication for such data. Upon receipt of data from the TOE, the peer external IT entity must be able to decrypt the data and verify that the received data accurately represents the data that was originally transmitted.
OE.PLACEMENT {IPS}	IPS must be placed in such a way to ensure adequate coverage of network segments where critical assets are located.

4.3 SECURITY OBJECTIVES RATIONALE

4.3.1 Coverage

The following table provides a mapping of TOE objectives to threats, showing that each TOE objective addresses at least one threat or organizational security policy.

	T.UNDETECTED	T.MEDIAT	T.ACCESS	T. FAILURE {Firewall/VPN}	T.DISCLOSE {Firewall/VPN}	T.MODIFY {Firewall/VPN}	P.MANAGE	P.HIDE {Firewall/VPN}	P.INSPECT {IPS}
O.AUDIT	X								
O.MANAGE			X				X		
O.MEDIAT		X							
O.AVAILABILITY {Firewall/VPN}				X					
O.HIDE {Firewall/VPN}								X	
O.CHANNEL {Firewall/VPN}					X	X			
O.INSPECT {IPS}									X

Table 1 Mapping of security objectives to threats and policies

The following table provides a mapping of the objectives for the operational environment to assumptions and threats, showing that each objective addresses at least one assumption or threat.

Objective	Assumptions / Threats
OE.ADMIN	A.ADMIN, T.ACCESS
OE.ADMINTRUST	A.ADMINTRUST
OE.AUDITMAN	A.AUDITMAN, T.UNDETECTED,
OE.AUDITSUPP	A.AUDITSUPP, T.UNDETECTED,
OE.MEDIATSUPP	A.MEDIATSUPP, T.MEDIAT
OE.ENVIRON	A.ENVIRON, T.ACCESS
OE.TIME	A.TIME, T.MEDIAT, T.UNDETECTED
OE.USERAUTH {Firewall/VPN}	A.USERAUTH {Firewall/VPN}, T.MEDIAT
OE.VPN {Firewall/VPN}	A.VPN {Firewall/VPN}

OE.PLACEMENT {IPS}	A.PLACEMENT {IPS}

Table 2 Mapping of security objectives for the operational environment to assumptions, threats and policies.

4.3.2 Sufficiency

The following rationale provides justification that the security objectives are suitable to counter each individual threat and satisfy each organizational security policy and that each security objective tracing back to a threat, when achieved, actually contributes to the removal, diminishing or mitigation of that threat or satisfying the organizational security policy.

Threat / OSP	Rationale for security objectives
T.UNDETECTED	A threat agent may attempt to compromise the assets without being detected. This threat includes a threat agent causing audit records to be lost or prevent future records from being recorded by taking actions to exhaust audit storage capacity, thus masking an attacker’s actions. This threat is diminished by: ▪ Audit records which record security relevant events (O.AUDIT), ▪ Security relevant events are prioritized and prevented as audit storage capacity fills (O.AUDIT), ▪ Administrator actions being auditable (OE.AUDITSUPP), ▪ An audit trail that can be effectively reviewed (OE.AUDITMAN), and ▪ Reliable timestamps being available for the audit trail (OE.TIME).
T.MEDIAT	An unauthorized person may send information through the TOE, which results in the exploitation and/or compromise of IT Assets. This threat includes an unauthorized person attempting to bypass the information flow control policy by sending an IP packet with a fake source address. This threat is diminished by: ▪ Applying the firewall security policy to all information that passes through the networks between users and external IT entities (O.MEDIAT and OE.MEDIATSUPP), ▪ Preventing information flow for any packet that uses the source routing option (O.MEDIAT), ▪ Ensuring that the TOE provides the only connection for information flow (OE.MEDIATSUPP), ▪ Reliable timestamps being available for time-based information flow control decisions (OE.TIME), and ▪ User authentication services available for information flow control decisions (Firewall/VPN only) (OE.USERAUTH {Firewall/VPN}).
T.ACCESS	An unauthorized person may read, access TOE management functions, and read, modify, or destroy security critical TOE data. This threat is diminished by: ▪ Providing a means for administrators to manage the security functions and trusted data (O.MANAGE), ▪ Ensuring that only administrators have TOE access (OE.ADMIN), ▪ Ensuring that the Management Servers and network used by the administrators are dedicated to the TOE usage (OE.ENVIRON).
T.FAILURE {Firewall/VPN}	A failure of a node or a network connection to a node caused by a threat agent or due to the normal lifecycle of components could cause denial of service making IT assets not available. This threat is diminished by: ▪ Providing high availability to information flow by the firewall cluster (O.AVAILABILITY {Firewall/VPN}).
T.DISCLOSE {Firewall/VPN}	Disclosure of information transmitted between the TOE and a remote trusted network by a threat on the external network connecting the TOE and the trusted network. This threat is addressed by the TOE providing a trusted channel

	(O.CHANNEL {Firewall/VPN}).
T.MODIFY {Firewall/VPN}	Undetected modification of information transmitted between the TOE and a remote trusted network by a threat on the external network connecting the TOE and the trusted network. This threat is addressed by the TOE providing a trusted channel (O.CHANNEL {Firewall/VPN}).
P.MANAGE	Management support of the TOE security functions is addressed by the security objectives of the TOE to be manageable (O.MANAGE).
P.HIDE {Firewall/VPN}	The TOE security function must be able to hide the IP addresses of hosts on the internal network and of the network topology of the internal network (O.HIDE {Firewall/VPN}).
P.INSPECT {IPS}	The inspection performed by the TOE of information flowing through the TOE to ensure that the information flow through the TOE is consistent with the applicable information flow control policies (O.INSPECT {IPS}).

Table 3 Sufficiency of objectives countering threats and satisfying the OSPs

The rationale for assumptions is done by a direct mapping of each assumption to a security objective for the environment with corresponding name and description, it is therefore self-explanatory.

Assumption	Rationale for security objectives
A.ADMIN	OE.ADMIN
A.ADMINTRUST	OE.ADMINTRUST
A.AUDITMAN	OE.AUDITMAN
A.AUDITSUPP	OE.AUDITSUPP
A.MEDIATSUPP	OE.MEDIATSUPP
A.ENVIRON	OE.ENVIRON
A.TIME	OE.TIME
A.USERAUTH {Firewall/VPN}	OE.USERAUTH {Firewall/VPN}
A.VPN {Firewall/VPN}	OE.VPN {Firewall/VPN}
A.PLACEMENT {IPS}	OE.PLACEMENT {IPS}

Table 4 Sufficiency of objectives holding assumptions

5 EXTENDED COMPONENTS DEFINITION

The extended functional security requirement, FAU_STG.NIAP-0414 is used for compliance with NIAP interpretation 0414. It imposes no additional assurance requirements. FAU_STG.NIAP-0414 has been used to express functionality configurable by the administrator related to prioritization of audit records when audit trail storage is full.

The extended requirements FCS_RBG_EXT.1 is taken from the NIAP Protection Profile for Network Devices [NDPP]. The extended functional security requirement FCS_IPSEC_EXT.1 is taken from the NIAP Protection Profile Network Device Protection Profile (NDPP) Extended Package VPN Gateway [NDPP-VPN].

5.1 FAU_STG – SECURITY AUDIT EVENT STORAGE

Family behavior

This family defines the requirements for the TSF to be able to create and maintain a secure audit trail. Stored audit records refer to those records within the audit trail, and not the audit records that have been retrieved (to temporary storage) through selection.

Component Leveling

FAU_STG.NIAP-0414 is hierarchically to component FAU_STG.4.

Management

The following actions could be considered for the management functions in FMT:

Maintenance (deletion, modification, addition) of actions to be taken in case of audit storage failure.

Audit

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ST:

1. Basic: Actions taken due to the audit storage failure.

2. Basic: Selection of an action to be taken when there is an audit storage failure.

5.1.1 FAU_STG.NIAP-0414 – Site-Configurable Prevention of Audit Loss

Hierarchical to:	FAU_STG.4
Dependencies:	FAU_STG.1 Protected Audit Trail Storage FMT_MTD.1 Management of TSF Data

FAU_STG.NIAP-0414-1

The TSF shall provide the administrator the capability to select one or more of the following actions [*selection: 'ignore auditable events', 'prevent auditable events, except those taken by the authorized user with special rights', 'overwrite the oldest stored audit records'*] and [*assignment: other actions to be taken in case of audit storage failure*] to be taken if the audit trail is full.

FAU_STG.NIAP-0414-2

The TSF shall [*selection: 'ignore auditable events', 'prevent auditable events, except those taken by the authorized user with special rights', 'overwrite the oldest stored audit records', assignment: other actions to be taken in case of audit storage failure*] if the audit trail is full and no other action has been selected.

Application Note: This component specifies the set of administrator selectable actions that the TSF must be capable of performing when the audit trail is full and allows the administrator to specify which action is to be performed by the TSF. It also provides a default action to take if the administrator does not select one of the actions.

5.2 FCS_IPSEC_EXT – CRYPTOGRAPHIC SUPPORT

Family behavior

The family FCS_IPSEC_EXT has been added to the FCS class to address the requirements of a secure trusted channel using IPsec. The set of the IPsec requirements specified here taken from the Network Device Protection Profile (NDPP) Extended Package VPN Gateway.

Component Leveling

FCS_IPSEC_EXT.1 is not hierarchically to any other component.

Management

There are no management activities foreseen.

Audit

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ST:

a. Minimum Session establishment with peer

5.2.1 FCS_IPSEC_EXT.1 – Internet protocol security (IPsec) communications

Hierarchical to: No other component

Dependencies: FCS_RBG_EXT.1 Random bit generator

FCS_IPSEC_EXT.1.1 The TSF shall implement the IPsec architecture as specified in RFC 4301.

FCS_IPSEC_EXT.1.2 The TSF shall implement [*selection, choose at least one of: tunnel mode, transport mode*].

PP Application Note: Future versions of this Extended Package will require that the TSF implement both tunnel mode and transport mode.

FCS_IPSEC_EXT.1.3 The TSF shall have a nominal, final entry in the SPD that matches anything that is otherwise unmatched, and discards it.

FCS_IPSEC_EXT.1.4 The TSF shall implement the IPsec protocol ESP as defined by RFC 4303 using the cryptographic algorithms AES-GCM-128, AES-GCM-256 as specified in RFC 4106, [*selection: AES-CBC- 128, AES-CBC-256 (both specified by RFC 3602) together with a Secure Hash Algorithm (SHA)-based HMAC, no other algorithms*].

PP Application Note: If an AES-CBC selection is made, the SHA-based HMAC must be consistent with what is specified in the NDPP FCS_COP.1(4) Cryptographic Operation (for keyed-hash message authentication) requirement.

FCS_IPSEC_EXT.1.5 The TSF shall implement the protocol: [*selection, choose at least one of: IKEv1 as defined in RFCs 2407, 2408, 2409, RFC 4109, [selection: no other RFCs for extended sequence numbers, RFC 4304 for extended sequence numbers] and [selection: no other RFCs for hash functions, RFC 4868 for hash functions]; IKEv2 as defined in RFCs 5996 (with mandatory support for NAT traversal as specified in section 2.23) and [selection: no other RFCs for hash functions, RFC 4868 for hash functions*]].

FCS_IPSEC_EXT.1.6 The TSF shall ensure the encrypted payload in the [*selection, choose at least one of: IKEv1, IKEv2*] protocol uses the cryptographic algorithms AES-CBC-128, AES-CBC-256 as specified in RFC 6379 and [*selection: AES-GCM-128, AES-GCM-256 as specified in RFC 5282, no other algorithm*].

FCS_IPSEC_EXT.1.7 The TSF shall ensure that IKEv1 Phase 1 exchanges use only main mode.

PP Application Note: Element 1.7 is only applicable if IKEv1 is selected.

FCS_IPSEC_EXT.1.8 The TSF shall ensure that [*selection: IKEv2 SA lifetimes can be configured by an Administrator based on number of packets or length of time, where the time values can be limited to: 24 hours for Phase 1 SAs and 8 hours for Phase 2 SAs, IKEv1 SA lifetimes can be configured by an Administrator based on number of packets or length of time, where the time values can be limited to: 24 hours for Phase 1 SAs and 8 hours for Phase 2 SAs*].

PP Application Note: It is appropriate to refine the requirement in terms of number of MB/KB instead of number of packets, as long as the TOE is capable of setting a limit on the amount of traffic that is protected by the same key (the total volume of all IPsec traffic protected by that key).

FCS_IPSEC_EXT.1.9 The TSF shall generate the secret value x used in the IKE Diffie-Hellman key exchange (“x” in g^x mod p) using the random bit generator specified in FCS_RBG_EXT.1, and having a length of at least [*assignment: (one or more) number(s) of bits that is at least twice the “bits of security” value associated with* *the negotiated Diffie-Hellman group as listed in Table 2 of NIST SP 800-57, Recommendation for Key Management – Part 1: General*] bits.

FCS_IPSEC_EXT.1.10 The TSF shall generate nonces used in IKE exchanges in a manner such that the probability that a specific nonce value will be repeated during the life a specific IPsec SA is less than 1 in 2^*[*assignment: (one or more) "bits of security" value(s) associated with the negotiated Diffie-Hellman group as listed in Table 2 of NIST SP 800-57, Recommendation for Key Management – Part 1: General*].

FCS_IPSEC_EXT.1.11 The TSF shall ensure that all IKE protocols implement DH Groups 14 (2048-bit MODP), 19 (256-bit Random ECP), and [*selection: 5 (1536-bit MODP), 24 (2048-bit MODP with 256-bit POS), 20 (384-bit Random ECP), [assignment: other DH groups that are implemented by the TOE], no other DH groups*].

FCS_IPSEC_EXT.1.12 The TSF shall ensure that all IKE protocols perform peer authentication using a [*selection, choose at least one of: RSA, ECDSA*] that use X.509v3 certificates that conform to RFC 4945 and [*selection: Pre-shared Keys, no other method*].

FCS_IPSEC_EXT.1.13 The TSF shall be able to ensure by default that the strength of the symmetric algorithm (in terms of the number of bits in the key) negotiated to protect the [*selection: IKEv1 Phase 1, IKEv2 IKE_SA*] connection is greater than or equal to the strength of the symmetric algorithm (in terms of the number of bits in the key) negotiated to protect the [*selection: IKEv1 Phase 2, IKEv2 CHILD_SA*] connection.

5.3 FCS_RBG_EXT – RANDOM BIT GENERATION

Family behavior

This family is part of the FCS class. It is intended to support the random bit generation, which is the basis for cryptographic key generation. This family should be included whenever there are functional requirements for the generation of random bits such as cryptographic keys.

Component Leveling

FCS_RBG_EXT.1.

Management

There are no management activities foreseen.

Audit

There are no auditable events foreseen.

5.3.1 FCS_RBG_EXT.1 – Cryptographic operation (Random bit generation)

Hierarchical to:	No other component
Dependencies:	No dependencies

FCS_RBG_EXT.1.1 The TSF shall perform all random bit generation (RBG) services in accordance with [*selection, choose one of: NIST Special Publication 800-90 using [selection: Hash_DRBG (any), HMAC_DRBG (any), CTR_DRBG (AES), Dual_EC_DRBG (any)*]; FIPS Pub 140-2 Annex C: X9.31 Appendix 2.4 using AES] seeded by an entropy source that accumulated entropy from [*selection, one or both of: a software-based noise source; a TSF-hardware-based noise source*].

FCS_RBG_EXT.1.2 The deterministic RBG shall be seeded with a minimum of [*selection, choose one of: 128 bits, 256 bits*] of entropy at least equal to the greatest bit length of the keys and authorization factors that it will generate.

Application Note: NIST Special Pub 800-90, Appendix C describes the minimum entropy measurement that will probably be required future versions of FIPS-140. If possible this should be used immediately and will be required in future versions of this PP.

For the first selection in FCS_RBG_EXT.1.1, the ST author should select the standard to which the RBG services comply (either 800-90 or 140-2 Annex C).

SP 800-90 contains four different methods of generating random numbers; each of these, in turn, depends on underlying cryptographic primitives (hash functions/ciphers). The ST author will select the function used (if 800-90 is selected), and include the specific underlying cryptographic primitives used in the requirement or in the TSS. While any of the identified hash functions (SHA-1, SHA-224, SHA-256, SHA-384, SHA-512) are allowed for Hash_DRBG or HMAC_DRBG, only AES-based implementations for CT_DRBG are allowed. While any of the curves defined in 800-90 are allowed for Dual_EC_DRBG, the ST author not only must include the curve chosen, but also the hash algorithm used.

For the second selection in FCS_RBG_EXT.1.1, the ST author indicates whether the sources of entropy are software-based, hardware-based, or both. If there are multiple sources of entropy, the ST will elaborate each entropy sources and whether it is hardware- or software-based. Hardware-based noise sources are preferred.

Note that for FIPS Pub 140-2 Annex C, currently only the method described in NIST-Recommended Random Number Generator Based on ANSI X9.31 Appendix A.2.4 Using the 3-Key Triple DES and AES Algorithms, Section 3 is valid. If the key length for the AES implementation used here is different than that used to encrypt the user data, then FCS_COP.1 may have to be adjusted or iterated to reflect the different key length. For the selection in FCS_RBG_EXT.1.2, the ST author selects the minimum number of bits of entropy that is used to seed the RBG.

The ST author also ensures that any underlying functions are included in the baseline requirements for the TOE.

6 SECURITY REQUIREMENTS

6.1 TOE SECURITY FUNCTIONAL REQUIREMENTS

The following are the conventions used for the operations applied to the Security Functional Requirements: Assignment, selection and refinement is indicated in **bold**. Iterations are indicated with a letter, e.g. FCS_COP.1a {Firewall/VPN}. Security functional requirements that are specific to the roles are indicated with a {Firewall/VPN} or {IPS} only, e.g. FDP_IFC.1 {Firewall/VPN} and FDP_IFC.2 {IPS}.

Class	Component	Component Name
Class FAU – Security audit		
	FAU_GEN.1	Security audit data generation
	FAU_SEL.1	Selective audit
	FAU_STG.1	Protected audit trail storage
	FAU_STG.NIAP-0414.1	Site-configurable prevention of audit loss
Class FCS – Cryptographic support		
	FCS_CKM.1a {Firewall/VPN}	Cryptographic key generation (for key establishment)
	FCS_CKM.1b {Firewall/VPN}	Cryptographic key generation (for IKE peer authentication)
	FCS_CKM.1c {Firewall/VPN}	Cryptographic key generation (symmetric keys)
	FCS_CKM.4 {Firewall/VPN}	Cryptographic key destruction
	FCS_COP.1a {Firewall/VPN}	Cryptographic operation (for data encryption/ decryption)
	FCS_COP.1b {Firewall/VPN}	Cryptographic operation (for cryptographic signature)
	FCS_COP.1c {Firewall/VPN}	Cryptographic operation (for cryptographic hashing)
	FCS_COP.1d {Firewall/VPN}	Cryptographic operation (for keyed-hash message authentication)
	FCS_IPSEC_EXT.1 {Firewall/VPN}	Internet protocol security (IPsec) communications
	FCS_RBG_EXT.1 {Firewall/VPN}	Random bit generation
Class FDP – User data protection		
	FDP_IFC.1 {Firewall/VPN}	Subset information flow control
	FDP_IFF.1 {Firewall/VPN}	Simple security attributes
	FDP_IFC.2 {IPS}	Subset information flow control
	FDP_IFF.1 {IPS}	Simple security attributes
Class FMT – Security management		

	FMT_MSA.1 {Firewall/VPN}
	FMT_MSA.1 {IPS}
		Management of security attributes

	FMT_MSA.2	Secure security attributes

	FMT_MSA.3 {Firewall/VPN}
	FMT_MSA.3 {IPS}
		Static attribute initialization

	FMT_MTD.1	Management of TSF data
	FMT_SMF.1	Specification of management functions

	FMT_SMR.1	Security roles
Class FPT – Protection of the TSF		
	FPT_FLS.1 {Firewall/VPN}	Failure with preservation of secure state
Class FRU – Resource utilization		
	FRU_FLT.2 {Firewall/VPN}	Limited fault tolerance

Table 5 Functional Components

6.1.1 Class FAU – Security audit

FAU_GEN.1 – Audit data generation

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

a) Start-up and shutdown of the audit functions;

b) All auditable events for the **not specified** level of audit; and

c) **the events in** Table 6**.**

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, **information specified in column three in** Table 6.

Functional Component	Auditable Event	Additional Audit Record Contents
FAU_STG.NIAP-0414	**Actions taken due to the audit storage failure.**	**None**
FDP_IFF.1 {Firewall/VPN}	**All decisions on requests for information flow except denial of packets with the IP source route option set, (i.e., the TOE denies all source route packets but does not record the denial in the audit log.)**	**Source IP address of request**
FDP_IFF.1 {IPS}	**All decisions on requests for information flow except denial of packets with the IP source route option set, (i.e., the TOE denies all source route packets but does not record the denial in the audit log.)**	**Source IP address of request**
FMT_SMF.1	**Use of the management functions. When a change is made via the Management Server, the Management Server generates audit records of this change. The TOE records that a change has been made and includes the identifier of the Management Server record.**	**Policy identifier (which is the reference to the management audit record.**
FPT_FLS.1	**Failure from security policy not being recognized, and loss of connectivity to user or management networks.**	**None**

Table 6 TOE Auditable Events

Application Note: For the TOE operating in the Firewall/VPN role the events of the FDP_IFF.1 {IPS} does not apply and for TOE operating in the IPS role the events of the FDP_IFF.1 {Firewall/VPN} does not apply in the table above.

FAU_SEL.1 – Selective audit

FAU_SEL.1.1 The TSF shall be able to select the set of events to be audited from the set of all auditable events based on the following attributes:

a) **user identity, subject identity, event type**

b) **all attributes used for the rules defined in FDP_IFF.1.1 except TOE interface on which traffic arrives.**

Application Note: The reference above to FDP_IFF.1.1 only applies to either the Firewall/VPN or the IPS instance of these requirements respectively.

FAU_STG.1 – Protected audit trail storage

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

FAU_STG.1.2 The TSF shall be able to **prevent** unauthorized modifications to the stored audit records in the audit trail.

FAU_STG.NIAP-0414 – Site-Configurable Prevention of Audit Loss

FAU_STG.NIAP-0414.1

The TSF shall provide the administrator the capability to select one or more of the following actions **prevent audited**[1] **events, except those taken by the authorized user with special rights** and **the capability to prioritize audited events that get spooled on the local node while space is available on the node:**

Alert:	**Generated with an alert status and are always stored.**
Essential:	**Always generated even if the TSF is running out of disk space.**
Stored:	**Stored to the audit log database if alert and essential log entries have already been stored.**
Transient:	**Not stored to database but kept in local log cache.**

to be taken if the audit trail is full.

Application Note: In the case of the IPS there is no clustering, so the node is always the local IPS.

FAU_STG.NIAP-0414.2

The TSF shall **prevent audited events, except those taken by the authorized user with special rights** if the audit trail is full and no other action has been selected.

6.1.2 Class FCS – Cryptographic support

FCS_CKM.1a {Firewall/VPN} – Cryptographic Key Generation (for key establishment)

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

- **NIST Special Publication 800-56A, “Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography” for elliptic curve-based key establishment schemes and implementing “NIST curves” ECDSA P- 256, P-384 and no other curves (as defined in FIPS PUB 186- 3, “Digital Signature Standard”)**
- **NIST Special Publication 800-56A, “Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography” for finite field-based key establishment schemes;**

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

[1] “auditable” is changed to “audited” in this component to make the NIAP interpretation consistent with a corresponding wording change in CC Version 3.1, Revision 4.

PP Application Note: This Extended Package requires specific algorithms to be used in key establishment, and this instantiation of the requirement from the NDPP ensures the right selections are made.

Application Note: These ephemeral asymmetric keys are used to compute the shared secret as described in section 5.7.1.1 Finite Field Cryptography Diffie-Hellman (FFC DH) Primitive and section 5.7.1.2 Elliptic Curve Cryptography Cofactor Diffie-Hellman (ECC CDH) Primitive in NIST Special Publication 800-56A.

FCS_CKM.1b {Firewall/VPN} – Cryptographic Key Generation (for IKE peer authentication)

FCS_CKM.1.1 The TSF shall generate **asymmetric** cryptographic keys **used for IKE peer authentication** in accordance with

- **FIPS PUB 186-3, “Digital Signature Standard (DSS)”, Appendix B.3.6 for RSA schemes;**
- **FIPS PUB 186-3, “Digital Signature Standard (DSS)”, Appendix B.4.1 for ECDSA schemes and implementing “NIST curves” P-256, P-384 and no other curves**

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

PP Application Note: The keys that are generated by the TOE through this requirement are intended to be used for the authentication of the VPN peers during the IKE (either v1 or v2) key exchange.

Application Note: The public keys that are generated are sent to the SMC with a “certificate signing requests” and turned into certificates by the SMC. These certificates are then used to authenticate the IKE peers for the establishment of VPN connections.

FCS_CKM.1c {Firewall/VPN} – Cryptographic Key Generation (symmetric keys)

FCS_CKM.1.1 The TSF shall generate **symmetric** cryptographic keys **used for IKE and IPsec protocols** in accordance with

- **NIST Special Publication 800-56A, “Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography” for key agreement using ephemeral keys and implementing FFC DH and ECC CDH primitives**
- **RFC 2409 for key derivation in the IKEv1 protocol and RFC 5996 for key derivation in the IKEv2 protocol.**

and specified cryptographic key sizes **128 and 256 bits.**

Application Note: The keys that are generated through this requirement are used in the IKE (either v1 or v2) key exchange for encryption/decryption of IKE messages (AES-CBC-128 and AES-CBC-256), for HMAC (IKE message authentication HMAC-SHA-256 and HMAC-SHA-356) as well as for IPsec data encryption/decryption (AES-GCM-128 and AES-GCM-256).

The following Key Establishment Schemes are used: FCC DH dhEphem, C(2, 0, FCC DH) and ECC CDH Ephemeral Unified Model, C(2, 0, ECC DH) defined in section 6 in NIST Special Publication 800-56A.

FCS_CKM.4 {Firewall/VPN} – Cryptographic key destruction

FCS_CKM.4.1 The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method **overwriting with zero** that meets the following: **no specific metric**.

Application Note: Keys are zeroized programmatically after use by the cryptographic modules and applications. Keys in volatile memory are also destroyed by power off and rebooting of the system.

FCS_COP.1a {Firewall/VPN} – Cryptographic Operation (for data encryption/decryption)

FCS_COP.1.1a The TSF shall perform **encryption and decryption** in accordance with a specified cryptographic algorithm **AES operating in GCM, CBC, and no other modes** and cryptographic key sizes **128-bits, 256-bits, and no other key sizes** that meets the following:

- **FIPS PUB 197, "Advanced Encryption Standard (AES)"**
- **NIST SP 800-38D, NIST SP 800-38A, no other standards**

PP Application Note: This Extended Package requires the modes GCM and CBC to be used in the IPsec and IKE protocols (FCS_IPSEC_EXT.1.4, FCS_IPSEC_EXT.1.6). Therefore, the FCS_COP.1.1(1) element in the NDPP has been specified here to ensure the ST Author includes these two modes to be consistent with the IPsec requirements.

Application Note: This requirement specifies encryption/decryption of IKE message (AES-CBC-128 and AES-CBC-256) and IPsec data (AES-GCM-128 and AES-GCM-256).

FCS_COP.1b {Firewall/VPN} – Cryptographic Operation (for cryptographic signature)

FCS_COP.1.1b The TSF shall perform **cryptographic signature services** in accordance with a:

- **RSA Digital Signature Algorithm (RSA) with a key size (modulus) of 2048 bits that meets FIPS PUB 186- 2 or FIPS PUB 186-3, "Digital Signature Standard",**
- **Elliptic Curve Digital Signature Algorithm (ECDSA) with key sizes of 256 and 384 bits that meet FIPS PUB 186-3, "Digital Signature Standard" with "NIST curves" P-256, P-384 and no other curves (as defined in FIPS PUB 186-3, "Digital Signature Standard").**

Application Note: RSASSA-PKCS-v1_5 signature scheme is used for RSA cryptographic signatures services as defined in [PKCS1v2.1].

FCS_COP.1c {Firewall/VPN} – Cryptographic Operation (for cryptographic hashing)

FCS_COP.1.1c The TSF shall perform **cryptographic hashing services** in accordance with a specified cryptographic algorithm **SHA-256 and SHA-384 and message digest sizes 256 and 384 bits** that meet the following: **FIPS Pub 180-3, "Secure Hash Standard."**

Application Note: This SFR has been taken from the NDPP in which it is called FCS_COP.1(3). The refinement and assignments have already been performed in the NDPP, and the selection of cryptographic algorithms have been restricted by the NDPP. Hash values are signed with FCS_COP.1b {Firewall/VPN}.

FCS_COP.1d {Firewall/VPN} – Cryptographic Operation (for keyed-hash message authentication)

FCS_COP.1.1d The TSF shall perform **keyed-hash message authentication** in accordance with a specified cryptographic algorithm **HMAC-SHA-256 and HMAC-SHA-384, key size 256 (in bits) used in HMAC, and message digest sizes 256 and 384 bits** that meet the following: **FIPS Pub 198-1, "The Keyed- Hash Message Authentication Code, and FIPS Pub 180-3, "Secure Hash Standard."**

Application Note: This SFR has been taken from the NDPP in which it is called FCS_COP.1(4). The refinement and assignments have already been performed in the NDPP, and the selection of cryptographic algorithms have been restricted by the NDPP. This SFR is used to ensure IKE (either v1 or v2) message authentication.

FCS_IPSEC_EXT.1 {Firewall/VPN} – Internet Protocol Security (IPsec) Communications

FCS_IPSEC_EXT.1.1 The TSF shall implement the IPsec architecture as specified in RFC 4301.

FCS_IPSEC_EXT.1.2 The TSF shall implement **tunnel mode**.

PP Application Note: Future versions of this Extended Package will require that the TSF implement both tunnel mode and transport mode.

FCS_IPSEC_EXT.1.3 The TSF shall have a nominal, final entry in the SPD that matches anything that is otherwise unmatched, and discards it.

FCS_IPSEC_EXT.1.4 The TSF shall implement the IPsec protocol ESP as defined by RFC 4303 using the cryptographic algorithms AES-GCM-128, AES-GCM-256 as specified in RFC 4106, **no other algorithms**.

PP Application Note: If an AES-CBC selection is made, the SHA-based HMAC must be consistent with what is specified in the NDPP FCS_COP.1(4) Cryptographic Operation (for keyed-hash message authentication) requirement.

FCS_IPSEC_EXT.1.5 The TSF shall implement the protocol: **IKEv1 as defined in RFCs 2407, 2408, 2409, RFC 4109***,* **no other RFCs for extended sequence numbers and RFC 4868 for hash functions; IKEv2 as defined in RFCs 5996 (with mandatory support for NAT traversal as specified in section 2.23) and RFC 4868 for hash functions**.

FCS_IPSEC_EXT.1.6 The TSF shall ensure the encrypted payload in the **IKEv1 and IKEv2** protocols uses the cryptographic algorithms AES-CBC-128, AES-CBC-256 as specified in RFC 6379 and **no other algorithm**.

FCS_IPSEC_EXT.1.7 The TSF shall ensure that IKEv1 Phase 1 exchanges use only main mode.

PP Application Note: Element 1.7 is only applicable if IKEv1 is selected.

FCS_IPSEC_EXT.1.8 The TSF shall ensure that **IKEv2 SA lifetimes can be configured by an Administrator based on number of kB or length of time, where the time values can be limited to: 24 hours for Phase 1 SAs and 8 hours for Phase 2 SAs, IKEv1 SA lifetimes can be configured by an Administrator based on number of kB or length of time, where the time values can be limited to: 24 hours for Phase 1 SAs and 8 hours for Phase 2 SAs**.

PP Application Note: It is appropriate to refine the requirement in terms of number of MB/KB instead of number of packets, as long as the TOE is capable of setting a limit on the amount of traffic that is protected by the same key (the total volume of all IPsec traffic protected by that key).

Application note: This extended component has been refined from the number of packages to kB, as allowed in the PP application note.

FCS_IPSEC_EXT.1.9 The TSF shall generate the secret value x used in the IKE Diffie-Hellman key exchange (“x” in g^x mod p) using the random bit generator specified in FCS_RBG_EXT.1, and having a length of at least **224 bits**.

FCS_IPSEC_EXT.1.10 The TSF shall generate nonces used in IKE exchanges in a manner such that the probability that a specific nonce value will be repeated during the life a specific IPsec SA is less than 1 in 2^**112**.

FCS_IPSEC_EXT.1.11 The TSF shall ensure that all IKE protocols implement DH Groups 14 (2048-bit MODP), 19 (256-bit Random ECP), **20 (384-bit Random ECP)** and **no other DH groups**.

FCS_IPSEC_EXT.1.12 The TSF shall ensure that all IKE protocols perform peer authentication using a **RSA and ECDSA** that use X.509v3 certificates that conform to RFC 4945 and **no other method**.

FCS_IPSEC_EXT.1.13 The TSF shall be able to ensure by default that the strength of the symmetric algorithm (in terms of the number of bits in the key) negotiated to protect the **IKEv1 Phase 1 and IKEv2 IKE_SA** connection is greater than or equal to the strength of the symmetric algorithm (in terms of the number of bits in the key) negotiated to protect the **IKEv1 Phase 2 and IKEv2 CHILD_SA** connection.

FCS_RBG_EXT.1 {Firewall/VPN} – Cryptographic operation (Random bit generation)

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

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

6.1.3 Class FDP – User data protection

FDP_IFC.1 {Firewall/VPN} – Subset information flow control

FDP_IFC.1.1 The TSF shall enforce the **Firewall Information Flow Control SFP** on

a) **subjects: IT entities on the internal or external networks that send and receive information through the TOE to one another, and human users;**

b) **information: connections over IP sent through the TOE from one subject to another;**

c) **operations: pass information and initiate the following services: NAT, authentication check, and opening related connections**.

FDP_IFC.2 {IPS} – Complete information flow control

FDP_IFC.2.1 The TSF shall enforce the **IPS Information Flow Control SFP** on

a) **subjects: IT entities on the internal or external networks that send and receive information through the TOE to one another;**

b) **information: connections over IP sent through the TOE from one subject to another;**

and all operations that cause that information to flow to and from subjects covered by the SFP.

FDP_IFC.2.2 The TSF shall ensure that all operations that cause any information in the TOE to flow to and from any subject in the TOE are covered by an information flow control SFP.

FDP_IFF.1 {Firewall/VPN} – Simple security attributes

FDP_IFF.1.1 The TSF shall enforce the **Firewall Information Flow Control SFP** based on the following types of subject and information security attributes:

a) **subject security attributes:**
- **presumed IP address;**
- **port number**
- **user identity**

b) **information security attributes:**
- **presumed IP address of source subject;**
- **presumed IP address of destination subject;**
- **TOE interface on which traffic arrives;**
- **transport layer protocol information**
- **service (protocol and port);**
- **time/date of service request**.

FDP_IFF.1.2 The TSF shall permit an information flow between a controlled subject and **another controlled subject** via a controlled operation if the following rules hold:

- **When the ‘matching part’ of the rules in the rule base matches the information security attribute values and the ‘action part’ of the matched rule is ‘allow’. The rules may be composed from all possible combinations of the values of the information security attributes, created by the administrator, and**
- **When the ‘matching part’ of the rules in the rule base matches the information security attribute values and the ‘action part’ of the matched rule is ‘allow’ and the ‘authentication matching’ defined in the rule, as specified in FDP_IFF.1.3, is successful. The rules may be composed from all possible combinations of the values of the information security attributes, created by the administrator, and**
- **When the ‘matching part’ of the rules in the rule base matches the information security attribute values and the ‘action part’ of the matched rule is ‘allow’ and option or match of the matched rule specifies ‘vpn’, and the ‘VPN matching’ rules defined in FDP_IFF.1.3 are successful. The rules may be composed from all possible combinations of the values of the information security attributes, created by the administrator**.

FDP_IFF.1.3 The TSF shall enforce the **following additional information flow control rules:**

- **Authentication matching – when a match in a rule requires authentication, if the user identity is successfully authenticated by the external authentication method defined in the rule, authentication matching will return a succeed to the rules defined in FDP_IFF.1.2 and FDP_IFF.1.5, else it will return a fail, and**
- **VPN matching – if the connection arrived from the VPN specified (via IP address) in the rule or if the TOE can send it via the specified VPN, VPN matching will return a succeed to the rule defined in FDP_IFF.1.2 and FDP_IFF.1.5, else it will return a fail, and**
- **Source route protection - the TOE shall reject requests in which the subject specifies the route in which information shall flow en route to the receiving subject.**
- **To support NAT, static IP address translation will translate the source and/or destination IP address to another IP address as defined in the rule.**
- **To support VPN, the TOE will attempt to initiate a VPN tunnel based on VPN option specified in the rule and definitions of VPN tunnels in the security policy.**
- **To support authentication matching, the TSF initiates a request to the authentication service specified by the rule to obtain the authentication of the identity.**
- **When configured, the TOE will redirect FTP packets, based on RFC 959, to a proxy type of software**
- **When configured, the TOE will redirect SMTP, based on RFC 5321, packets to a proxy type of software,**
- **When configured, the TOE will redirect HTTP, based on RFC 2616, packets to a proxy type of software.**

FDP_IFF.1.4 The TSF shall explicitly authorise an information flow based on the following rules: **no explicit authorisation rules**.

FDP_IFF.1.5 The TSF shall explicitly deny an information flow based on the following rules:

- **When the ‘matching part’ of the rules in the rule base matches the information security attribute values and the ‘action part’ of the matched rule is ‘discard’ or ‘refuse’. The rules may be composed from all possible combinations of the values of the information security attributes, created by the administrator; and**
- **When the ‘matching part’ of the rules in the rule base matches the information security attribute values and the ‘authentication matching’ is defined in the rule, as specified in FDP_IFF.1.3, fails. The rules may be composed from all possible combinations of the values of the information security attributes, created by the administrator; and**
- **When the ‘matching part’ of the rules in the rule base matches the information security attribute values and the option or match of the matched rule specifies ‘vpn’, and the ‘VPN matching’ rules defined in FDP_IFF.1.3 fail. The rules may be composed from all possible combinations of the values of the information security attributes, created by the administrator; and**
- **The following rules can be deduced from the above rules but are explicitly included for clarity:**
    - **The TOE shall reject requests for access or services where the information arrives on an external TOE interface, and the presumed address of the source subject is an external IT entity on an internal network;**
    - **The TOE shall reject requests for access or services where the information arrives on an internal TOE interface, and the**

presumed address of the source subject is an external IT entity on the external network;

- **The TOE shall reject requests for access or services where the information arrives on either an internal or external TOE interface, and the presumed address of the source subject is an external IT entity on a broadcast network;**
- **The TOE shall reject requests for access or services where the information arrives on either an internal or external TOE interface, and the presumed address of the source subject is an external IT entity on the loopback network**.

FDP_IFF.1 {IPS} – Simple security attributes

FDP_IFF.1.1 The TSF shall enforce the **IPS Information Flow Control SFP** based on the following types of subject and information security attributes:

a) **subject security attributes:**

- **presumed IP address;**
- **port number**

b) **information security attributes:**

- **Ethernet frame type**
- **IPv4 payload**
    - **presumed IP address of source subject;**
    - **presumed IP address of destination subject;**
    - **TOE interface on which traffic arrives;**
    - **transport layer protocol information**
    - **service (protocol and port);**
- **payload (application layer data).**

FDP_IFF.1.2 The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold:

- **the Ethernet rules allow the information flow based on the Ethernet frame type;**
- **if the connection is not an existing TCP/IP connection permitted by the TSF, the following IPS Access Control rules are applied:**
    - **presumed IP address of source subject;**
    - **presumed IP address of destination subject;**
    - **TOE interface on which traffic arrives;**
    - **transport layer protocol information**
    - **service (protocol and port);**
- **the inspection rule of the specific application layer of the payload.**

FDP_IFF.1.3 The TSF shall enforce the **no further rule**.

FDP_IFF.1.4 The TSF shall explicitly authorize an information flow based on the following rules: **none**.

FDP_IFF.1.5 The TSF shall explicitly deny an information flow based on the following rules:

- **When the 'matching part' of the rules in the rule base matches the information security attribute values and the 'action part' of the matched rule is 'discard' or 'refuse'. The rules may be composed from all possible combinations of the values of the information security attributes, created by the administrator**.

6.1.4 Class FMT – Security Management

FMT_MSA.1 {Firewall/VPN} – Management of security attributes

FMT_MSA.1.1 The TSF shall enforce the **Firewall Information Flow Control SFP** to restrict the ability to **modify** the security attributes

a) **Attributes from a rule in the Firewall Information Flow Control SFP;**

b) **The rules in the Firewall Information Flow Control SFP**.

to **the Management Server**.

FMT_MSA.1 {IPS} – Management of security attributes

FMT_MSA.1.1 The TSF shall enforce the **IPS Information Flow Control SFP** to restrict the ability to **modify** the security attributes

a) **Attributes from a rule in the IPS Information Flow Control SFP;**

b) **The rules in the IPS Information Flow Control SFP**.

to **the Management Server**.

FMT_MSA.2 – Secure security attributes

FMT_MSA.2.1 The TSF shall ensure that only secure values are accepted for **all security attributes**.

Application Notes: The secure values for the security attributes applies both to the Firewall/VPN as well as to the IPS, although they are different sets of security attributes.

FMT_MSA.3 {Firewall/VPN} – Static attribute initialization

FMT_MSA.3.1 The TSF shall enforce the **Firewall Information Flow Control SFP** to provide **restrictive** default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2 The TSF shall allow the **none** to specify alternative initial values to override the default values when an object or information is created.

Application Notes: It is not possible for any user role to specify alternative initial values.

FMT_MSA.3 {IPS} – Static attribute initialization

FMT_MSA.3.1 The TSF shall enforce the **IPS Information Flow Control SFP** to provide **restrictive** default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2 The TSF shall allow the **none** to specify alternative initial values to override the default values when an object or information is created.

Application Notes: It is not possible for any user role to specify alternative initial values.

FMT_MTD.1 – Management of TSF data

FMT_MTD.1.1 The TSF shall restrict the ability to **access** the **data list in** Table 7 to **roles in** Table 7.

TOE Role	TSF DATA	Management Server
Firewall/VPN	**Auditable events, log levels, and log spool policy**	**Modify**
Firewall/VPN	**Security policy attributes**	**Modify**
Firewall/VPN	**NAT IP address translation table**	**Modify**
Firewall/VPN	**Actions to be taken in case of audit storage failure;**	**Modify**
Firewall/VPN	**For cluster definition for high availability including:** • **Interface data: NIC number mapping the interface number to the physical network address, CVI, NDI internal IP address and mask, NDI specifying interface network type (management, heartbeat, outgoing);** • **Network element data: cluster name, Log server ID;** **Routing information.**	**Modify, delete**

Firewall/VPN	**VPN channels and characteristics of the VPN channel**	**Add, delete, modify**
IPS	**Auditable events, log levels, and log spool policy**	**Modify**
IPS	**Actions to be taken in case of audit storage failure**	**Modify**
IPS	**IPS Ethernet, access control and inspection rules**	**Modify**

Table 7 TSF Data Management

FMT_SMF.1 – Specification of Management Functions

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

a) **Defining auditable events for information flow control auditing;**

b) **Defining Log Spool Policy;**

c) **Modifying log levels;**

d) **Modifying actions to be taken in case of audit storage failure;**

e) **Configuring access for Management Server interface for administrator;**

For the Firewall/VPN role, the following functions are also available:

f) **Configuring cluster definition for high availability with the following:**

- **Interface data: NIC number mapping the interface number to the physical network address, CVI, NDI internal IP address and mask, NDI specifying interface network type (management, heartbeat, outgoing);**
- **Network element data: cluster name, Log server ID**
- **Routing information.**

g) **Configuring Firewall Information Flow policy including NAT and authentication matching**.

h) **VPN channels and characteristics of the VPN channel (add, delete, modify)**

For the IPS role, the following functions are also available:

i) **Configuring IPS network element definition with the following:**

- **Interface data: NIC number mapping the interface number to the physical network address, logical interface pair for the flow between internal and external networks, NDI internal IP address and mask for the management interface;**
- **Network element data: name, Log server ID**
- **Routing information for management the interface.**

j) **Configuring IPS Information Flow policy including Ethernet rules, access control and inspection**.

FMT_SMR.1 – Security roles

FMT_SMR.1.1 The TSF shall maintain the roles **Management Server**.

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

6.1.5 Class FPT – Protection of the TSF

FPT_FLS.1 {Firewall/VPN} – Failure with preservation of secure state

FPT_FLS.1.1 The TSF shall preserve a secure state when the following types of failures occur:

a) **node power failure;**

b) **security policy not recognized;**

c) **interface to internal, external, management or cluster networks fails**.

6.1.6 Class FRU – Resource utilisation

FRU_FLT.2 {Firewall/VPN} – Limited fault tolerance

FRU_FLT.2.1 The TSF shall ensure the operation of all the TOE's capabilities when the following failures occur:

a) **power failure of cluster node;**

b) **security policy not recognized;**

c) **interface to internal, external, management or cluster networks fails**.

Application Notes: Power failure is only detected for other nodes in a cluster which the TOE is part of. The TOE cannot detect the power failure of itself, but if it is part of a cluster the other nodes of that cluster will detect it.

6.2 SECURITY FUNCTIONAL REQUIREMENTS RATIONALE

6.2.1 Coverage

The following table provides a mapping of SFR to the security objectives, showing that each security functional requirement addresses at least one security objective.

Requirement(s)	Objective(s)
FAU_GEN.1	O.AUDIT
FAU_SEL.1	O.AUDIT
FAU_STG.1	O.AUDIT
FAU_STG.NIAP-0414	O.AUDIT
FCS_CKM.1a {Firewall/VPN}	O.CHANNEL {Firewall/VPN}
FCS_CKM.1b {Firewall/VPN}	O.CHANNEL {Firewall/VPN}
FCS_CKM.1c {Firewall/VPN}	O.CHANNEL {Firewall/VPN}
FCS_CKM.4 {Firewall/VPN}	O.CHANNEL {Firewall/VPN}
FCS_COP.1a {Firewall/VPN}	O.CHANNEL {Firewall/VPN}
FCS_COP.1b {Firewall/VPN}	O.CHANNEL {Firewall/VPN}
FCS_COP.1c {Firewall/VPN}	O.CHANNEL {Firewall/VPN}
FCS_COP.1d {Firewall/VPN}	O.CHANNEL {Firewall/VPN}
FCS_IPSEC_EXT.1 {Firewall/VPN}	O.CHANNEL {Firewall/VPN}
FCS_RBG_EXT.1 {Firewall/VPN}	O.CHANNEL {Firewall/VPN}
FDP_IFC.1 {Firewall/VPN}	O.MEDIAT, O.HIDE {Firewall/VPN}
FDP_IFC.2 {IPS}	O.MEDIAT, O.INSPECT {IPS}
FDP_IFF.1 {Firewall/VPN}	O.MEDIAT, O.HIDE {Firewall/VPN}
FDP_IFF.1 {IPS}	O.MEDIAT, O.INSPECT {IPS}
FMT_MSA.1 {Firewall/VPN} and FMT_MSA.1 {IPS}	O.MANAGE
FMT_MSA.2	O.MANAGE
FMT_MSA.3 {Firewall/VPN} and FMT_MSA.3 {IPS}	O.MANAGE
FMT_MTD.1	O.MANAGE
FMT_SMF.1	O.MANAGE
FMT_SMR.1	O.MANAGE
FPT_FLS.1 {Firewall/VPN}	O.AVAILABILITY {Firewall/VPN}

FRU_FLT.2 {Firewall/VPN}	O.AVAILABILITY {Firewall/VPN}

Table 8 Mapping of security functional requirements to security objectives

6.2.2 Sufficiency

The following rationale provides justification for each security objective for the TOE, showing that the security functional requirements are suitable to meet and achieve the security objectives:

Objective	Security functional requirements rationale
O.AUDIT	The TOE must provide a means to accurately detect and record security-relevant events in audit records, and prevent audit data loss by prioritizing and preventing security-relevant events when the audit storage capacity fills. This objective is satisfied by requiring the following: ▪ An audit record can be generated for security-relevant events (FAU_GEN.1), ▪ Unauthorized deletion of audit records is prevented (FAU_STG.1), ▪ Security-relevant events can be included or excluded from the audit log based on selected attributes, and can be prioritized when the audit storage nears capacity (FAU_SEL.1 and FAU_STG.NIAP-0414), and When the audit log is full, auditable events are prevented from occurring (FAU_STG.NIAP-0414).
O.AVAILABILITY {Firewall/VPN}	The TOE when operating as part of a firewall cluster must provide high availability of information flow control, ensuring continuation of service when firewall nodes or their interfaces fail. This objective is satisfied by requiring a secure state is preserved and ensuring operation, when node hardware malfunctions, the security policy is not recognized, or there is a failure on the internal, external or cluster network interfaces (FRU_FLT.2 {Firewall/VPN}, and FPT_FLS.1 {Firewall/VPN}).
O.MANAGE	The TOE must provide a means for an administrator via the Management Server to manage the TOE security functions. This objective is satisfied by requiring there to be security management functions for the administrative roles (FMT_SMF.1 and FMT_SMR.1), and protection of the related trusted data and attributes (FMT_MSA.1 {IPS} and FMT_MSA.1 {Firewall/VPN}, FMT_MSA.2, FMT_MSA.3 {IPS} and FMT_MSA.3 {Firewall/VPN}, FMT_MTD.1).
O.MEDIAT	The TOE must mediate the flow of all information between users and external IT entities on the internal and external networks connected to the TOE in accordance with its security policy. This objective is satisfied by requiring a firewall security policy to control the information flow (FDP_IFC.1 {Firewall/VPN}, FDP_IFF.1 {Firewall/VPN}, FDP_IFC.2 {IPS} and FDP_IFF.1 {IPS}), and requiring that the policy is applied to all traffic between the internal and external interfaces.
O.HIDE {Firewall/VPN}	The TOE must provide a means to hide the IP addresses of hosts on its internal network. This objective is satisfied by requiring a firewall security policy that provides IP address translation services (FDP_IFC.1 {Firewall/VPN} and FDP_IFF.1 {Firewall/VPN}).
O.CHANNEL {Firewall/VPN}	The TOE must be able to provide trusted channels to remote trusted networks and protect information transmitted to and received from such networks against unauthorised disclosure and to detect any modification of incoming information transmitted from such networks, and to provide the means for the remote network to verify the integrity of information transmitted out of the TOE to such networks. This is satisfied by FCS_COP.1a {Firewall/VPN} (FCS_IPSEC_EXT.1.4 {Firewall/VPN}), which provides encryption, decryption and authentication of the IPsec payload. Keys for encryption, decryption and authentication of

	IPsec payload are generated using FCS_CKM.1c {Firewall/VPN} (that uses ephemeral keys generated using FCS_CKM.1a {Firewall/VPN}). FCS_COP.1a {Firewall/VPN} (FCS_IPSEC_EXT.1.6) provides encryption of IKE messages (keys are generated using FCS_CKM.1c {Firewall/VPN}), FCS_COP.1d {Firewall/VPN} provides IKE message authentication (keys for HMAC-SHA are generated using FCS_CKM.1c {Firewall/VPN}). FCS_CKM.1b {Firewall/VPN} generates signature keys for IKE peer authentication, FCS_COP.1b {Firewall/VPN} provides signature services and FCS_COP.1c {Firewall/VPN} provides hashes for signatures. The key generation is further supported by the random bit generation FCS_RBG_EXT.1 {Firewall/VPN} and by the key destruction FCS_CKM.4 {Firewall/VPN}.
O.INSPECT {IPS}	The TOE must be able to perform inspection of the information flowing through the TOE and enforce that any information flow allowed through is consistent with the applicable information flow control policies. This is satisfied by the complete information flow control FDP_IFC.2 {IPS} using an information flow control policy with the subject security attributes and information security attributes that are specified in FDP_IFF.1 {IPS}, to enforce the Ethernet rules and the IPS Access Control rules.

Table 9 Security objectives for the TOE rationale

6.2.3 Security Requirements Dependency Analysis

The following table demonstrates the dependencies of SFRs modeled in CC Part 2 and how the SFRs for the TOE resolve those dependencies:

SFR	Dependencies	Resolution
FAU_GEN.1	FPT_STM.1	IT-Environment (OE.TIME)
FAU_SEL.1	FAU_GEN.1	FAU_GEN.1
	FMT_MTD.1	FMT_MTD.1
FAU_STG.1	FAU_GEN.1	FAU_GEN.1
FAU_STG.NIAP-0414	FMT_MTD.1	FMT_MTD.1
	FAU_STG.1	FAU_STG.1 and IT-Environment (OE.AUDITSUPP)

FCS_CKM.1a {Firewall/VPN}	[FCS_CKM.2, or FCS_COP.1]
	FCS_CKM.4
		No, addressed by FCS_RBG_EXT.1 {Firewall/VPN}
		FCS_CKM.4 {Firewall/VPN}

FCS_CKM.1b {Firewall/VPN}	[FCS_CKM.2, or FCS_COP.1]
	FCS_CKM.4
		No, addressed by FCS_RBG_EXT.1 {Firewall/VPN}
		FCS_CKM.4 {Firewall/VPN}

FCS_CKM.1c {Firewall/VPN}	[FCS_CKM.2, or FCS_COP.1]
	FCS_CKM.4
		No, addressed by FCS_RBG_EXT.1 {Firewall/VPN} and FCS_CKM.1a {Firewall/VPN}
		FCS_CKM.4 {Firewall/VPN}

FCS_CKM.4 {Firewall/VPN}	[FDP_ITC.1, or FDP_ITC.2, or FCS_CKM.1]	FCS_CKM.1a {Firewall/VPN}, FCS_CKM.1b {Firewall/VPN} and FCS_CKM.1c {Firewall/VPN}

FCS_COP.1a {Firewall/VPN}	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1]
	FCS_CKM.4
		FCS_CKM.1c {Firewall/VPN}
		FCS_CKM.4 {Firewall/VPN}

FCS_COP.1b {Firewall/VPN}	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1]	FCS_CKM.1b {Firewall/VPN}
		FCS_CKM.4 {Firewall/VPN}

SFR	Dependencies	Resolution
	FCS_CKM.4	
FCS_COP.1c {Firewall/VPN}	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1] FCS_CKM.4	No, no keys are generated or imported because hashing services work without using keys.

FCS_COP.1d {Firewall/VPN}	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1]
	FCS_CKM.4
		FCS_CKM.1c {Firewall/VPN}
		FCS_CKM.4 {Firewall/VPN}

FCS_IPSEC_EXT.1 {Firewall/VPN}	FCS_RBG_EXT.1	FCS_RBG_EXT.1 {Firewall/VPN}
FCS_RBG_EXT.1 {Firewall/VPN}	None	–
FDP_IFC.1 {Firewall/VPN}	FDP_IFF.1	FDP_IFF.1 {Firewall/VPN}
FDP_IFF.1 {Firewall/VPN}	FDP_IFC.1	FDP_IFC.1 {Firewall/VPN}
	FMT_MSA.3	FMT_MSA.3
FDP_IFC.2 {IPS}	FDP_IFF.1	FDP_IFF.1 {IPS}
FDP_IFF.1 {IPS}	FDP_IFC.1	FDP_IFC.2 {IPS}
	FMT_MSA.3	FMT_MSA.3
FMT_MSA.1 {Firewall/VPN}	FDP_ACC.1 or FDP_IFC.1	FDP_IFC.1 {Firewall/VPN}
	FMT_SMR.1	FMT_SMR.1
	FMT_SMF.1	FMT_SMF.1
FMT_MSA.1 {IPS}	FDP_ACC.1 or FDP_IFC.1	FDP_IFC.2 {IPS}
	FMT_SMR.1	FMT_SMR.1
	FMT_SMF.1	FMT_SMF.1
FMT_MSA.2	FDP_ACC.1 or FDP_IFC.1	FDP_IFC.1 {Firewall/VPN} and FDP_IFC.2 {IPS}
	FMT_MSA.1	FMT_MSA.1 {Firewall/VPN} and FMT_MSA.3 {IPS}
	FMT_SMR.1	FMT_SMR.1
FMT_MSA.3 {Firewall/VPN}	FMT_MSA.1	FMT_MSA.1 {Firewall/VPN}
	FMT_SMR.1	No role can change the default values, so no such dependency exists.
FMT_MSA.3 {IPS}	FMT_MSA.1	FMT_MSA.1 {IPS}
	FMT_SMR.1	No role can change the default values, so no such dependency exists.
FMT_MTD.1	FMT_SMR.1	FMT_SMR.1
	FMT_SMF.1	FMT_SMF.1
FMT_SMF.1	None	–
FMT_SMR.1	FIA_UID.1	IT-Environment (OE.ADMIN)
FPT_FLS.1 {Firewall/VPN}	None	–
FRU_FLT.2 {Firewall/VPN}	FPT_FLS.1	FPT_FLS.1 {Firewall/VPN}

Table 10 TOE SFR dependency analysis

6.3 TOE SECURITY ASSURANCE REQUIREMENTS

The target Evaluation Assurance Level for this TOE is EAL4 augmented by ALC_FLR.1.

6.4 SECURITY ASSURANCE REQUIREMENTS RATIONALE

The evaluation assurance requirements were selected from an EAL to provide a balanced level assurance and to be appropriate with this assurance level for this type of product and consistent with the security objectives of the TOE, the TOE should withstand an attacker with an attack potential of Enhanced-Basic.

The Common Criteria authors have ensured that EAL4 is a sound selection of assurance components where all dependencies have been resolved. Since the augmentation of ALC_FLR.1 does not have any dependencies, there is no need to verify the consistency of the assurance component selection.

7 TOE SUMMARY SPECIFICATION

7.1 AUDIT

7.1.1 Audit Selection and Generation

The TOE provides an audit mechanism that cannot be disabled. The startup and shutdown of the audit function is synonymous with the start-up and shutdown of the TOE. The set of potential audit events and record information are defined in FAU_GEN.1.

The audit mechanism is the ‘logging’ operation which is triggered using the logging option of a rule in the TOE security policy. The TOE applies the matching mechanism for packet filtering, and for each match a logging option can be defined that generates an audit record. The TSF selects the audited events based on the defined logging options. In addition to the logging operation, the TOE provides an audit record when the TOE security policy (i.e., active file) changes. When the TOE receives a new security policy it generates an audit record identifying the date, time, and configuration identification. Note: the audit record generated by the TOE for component FMT_SMF.1 provides the link between the two sets of audit records.

The TOE relies on the operating system to provide the time for the audit records and for the Management Server to generate audit records providing the details on the use of the security management functions.

This TSF is mapped to the following SFRs: FAU_GEN.1, FAU_SEL.1

7.1.2 Preventing audit data loss

The TOE provides a mechanism to prevent audit data loss. TOE audit entries are first stored on cache buffers on each node. The size of this cache depends on the size of the hard disk. The proprietary protocol for synchronizing and managing the data among the distributed components notifies the Log Server that there is new log information and sends the log entry to the Log Server. The log information is stored by the Log Server as database files which are only accessible to a TOE administrator via the Management Server. An audit entry is removed from cache buffers after the TOE has received confirmation from Log Server that the entry has been successfully stored.

The administrator defines the log spool policy. This specifies the behavior of the TOE whenever its local log spool is filled as one of the following:

- Stop traffic (required in the evaluated configuration): TOE automatically goes to an offline state and connections going through TOE are transferred to other nodes in a cluster (please see information on high availability). Once the spool situation has improved, the node returns automatically to online state.
- Discard log: (the default setting and needs to be changed to the evaluated configuration) the TOE overlooks new log entries without any means of retrieval. This log spooling policy should be used only if the traffic is more important than the logs.

The TOE also provides a means for the Management Server to prioritize log data. The mechanism is based on the following log level:

Alert: generated with an alert status and are always stored;

Essential: always generated even if the Stonesoft Firewall/VPN & IPS Security Engine is running out of disk space;

Stored: stored to the audit log database if alert and essential log entries have already been stored;

Transient: not stored to database but kept in TOE log cache.

Before applying the selected log spooling policy, the engine stops producing transient logs. If insufficient, it can drop all but the essential log entries. As a last resort, the engine applies the selected log spooling policy.

This TSF is mapped to the following SFRs: FAU_STG.1, FAU_STG.NIAP-0414.1

7.2 MANAGEMENT FUNCTIONS

7.2.1 Management of TOE functions and data

Security management defines the protection and management mechanisms of the TOE. The management interface to the TOE is via the Management Server (a non-human user from the TOE perspective). This interface provides the functionality required for administrators to manage the trusted data and security attributes for the security functions. The TOE maintains a single role, Management Server, and the use of its interface implicitly defines the role.

The TOE implements consistency checking on the trusted data received through the Management Server interface to ensure only consistent values are accepted. A user must successfully be identified and authenticated by first logging into the Management Server to modify the configuration. Since the identification and authentication is performed by the Management Server, these security functions are therefore outside of the scope of the TOE.

These features are configurable for the Firewall/VPN:

1. Auditable events, log levels, and log spool policy (modify)
2. Actions to be taken in case of audit storage failure (modify)
3. Security policy attributes (modify)
4. NAT IP address translation table (modify)
5. For cluster definition for high availability (modify, delete):
    a. Interface data: NIC number mapping the interface number to the physical network address, CVI, NDI internal IP address and mask, NDI specifying interface network type (management, heartbeat, outgoing);
    b. Network element data: cluster name, Log server ID;
    c. Routing information.
6. VPN channels and characteristics of the VPN channel (add, delete, modify)

The TOE enforces restrictive default values for information flow security attributes. Any traffic that is not explicitly accepted by the security policy is rejected by the TOE in the Firewall/VPN role. The TSF applies the security policy to restrict the ability to modify the security attributes and the TSF data to the Management Server. An authorized human administrator must successfully log into the Management Server to modify the configuration to permit the flow of information.

These features are configurable for the IPS:

1. Auditable events, log levels, and log spool policy (modify)
2. Actions to be taken in case of audit storage failure (modify)
3. Security policy attributes (modify)
    a. Ethernet rules
    b. Access control policy
    c. Inspection rules
4. For IPS element definition (modify, delete):
    a. Interface data: NIC number mapping the interface number to the physical network address, logical interface pair for the flow between internal and external networks, NDI internal IP address and mask for the management interface;
    b. Network element data: name, Log server ID;
    c. Routing information for the management interface.

The inspection rules for IPS may be updated on a regular basis as new protocols and attack patterns are being known. Stonesoft provides subscriptions to an update services, but this is outside of the scope of the TOE and this ST.

This TSF is mapped to the following SFRs: FMT_MSA.1 {Firewall/VPN}, FMT_MSA.1 {IPS}, FMT_MSA.2, FMT_MSA.3 {Firewall/VPN}, FMT_MSA.3 {IPS}, FMT_MTD.1, FMT_SMF.1, FMT_SMR.1.

7.3 FIREWALL/VPN FUNCTIONS

The TSFs described in this section are only available to the TOE in the Firewall/VPN role.

7.3.1 Information flow control

The TOE provides an information flow control mechanism using a rule base that comprises a set of security policy rules, i.e., the firewall security policy. The TSF applies the firewall security policy to all traffic that passes through via its internal or external network interfaces. The traffic is TCP, UDP, ICMP, IPSec connections over IP. The TSF only permits traffic to pass through that has been explicitly allowed by the firewall security policy, and implements packet defragmentation to enforce the policy on entire IP packets. Administrators using the Management Server define the firewall security policy rules.

The TSF implements connection tracking to manage the information flow control decisions for connections rather than packets, providing increased performance and support for firewall features that require packet information above the IP level. The connection tracking mechanism stores the state information of each connection to allow packets belonging to an established connection to pass.

Connection tracking works closely with the protocol agents to manage the information flow control decisions based on information attributes at the different networking layers through the application layer to decide whether a packet should be granted access or not. The following protocol agents and their security function are within the scope of the evaluation: FTP, HTTP, and SMTP redirection.

The TSF follows a specific orderly algorithm to traverse the rule base for matching and filtering the traffic between its internal and external networks. Any traffic that is not explicitly accepted by the security policy is rejected by the firewall. The structure of the rule base and the capabilities of its associated protocol agents enable the TSF to make the information flow control decisions defined in FDP_IFF.1.2 {Firewall/VPN} through FDP_IFF.1.5 {Firewall/VPN}.

Each rule comprises matching criteria and target actions. If the matching criteria is verified (i.e., a comparison matches) the TSF applies the target actions. The TSF compares the information attributes defined in FDP_IFF.1.1 {Firewall/VPN} with the matching criteria of the rule to determine whether apply the rule. If applied the target actions are implemented and the additional capabilities and flow control rules defined in FDP_IFF.1.2 {Firewall/VPN} through FDP_IFF.1.5 {Firewall/VPN} are applied.

The rulebase is read from top down, and when the first matching rule is encountered the search stops and the TOE executes the matching rule. There are two exceptions to this:

a) jump rule - this makes the search jump to a sub-rulebase if the jump rule matches. The search will continue inside the sub-rulebase until it either finds a matching rule or comes back empty-handed from the sub-rulebase and continues searching through the main rulebase;

b) continue rule - when it matches, it will set some variables and then the search continues.

The matching criteria may require users to authenticate to the TOE before information can flow between the internal and external networks. The TOE relies on the IT environment to provide a user directory and a user authentication mechanism for user identity based information flow control.

The TOE relies on the operating system to provide the time for making the control decisions on the time-based information flow.

This TSF is mapped to the following SFRs: FDP_IFC.1 {Firewall/VPN}, FDP_IFF.1 {Firewall/VPN}

7.3.2 Network Address Translation (NAT)

When configured for static mapping NAT, the TOE provides a mechanism to ensure the real addresses on the internal networks are hidden. Static mapping is a one to one mapping and provides a means to determine the IP address number that is chosen.

Activation of NAT is done per connection based on the rule base. The TOE rewrites the headers of IP packets. It is a two-way process and keeps track of the source and destination addresses and can do a reverse translation to returning packets.

The NAT manipulation occurs after a connection has been accepted so that connection decisions are based on the original addresses. Routing takes place after the connection has been modified. NAT rules can be defined independently of access rules.

This TSF is mapped to the following SFRs: FDP_IFC.1 {Firewall/VPN}, FDP_IFF.1 {Firewall/VPN}

7.3.3 High availability

As part of a firewall cluster the TOE provides high availability of the firewall security services defined in the firewall security policy. Up to 16 firewall nodes can form a cluster. The evaluated configuration assumes the cluster uses a dedicated and secure network. In case a firewall node in a cluster has a power failure, or can't recognize its security policy, or a failure of an interface to an internal, external, management or cluster network, the firewall engine is capable of failing over all sessions to other nodes. This provides continuous enforcement of the firewall security policy including information flow control.

The TOE's clustering subsystem implements the high availability security feature. The clustering subsystem includes a set of proprietary protocols to communicate among the nodes of a cluster to communicate the following state information:

- Which nodes are online;
- What is the capacity of each online node;
- What is the load of each node;
- The following firewall state is exchanged:
  - Current connections
  - Active authentications

This TSF is mapped to the following SFRs: FPT_FLS.1 {Firewall/VPN}, FRU_FLT.2 {Firewall/VPN}

7.3.4 Cryptographic functionality

The TOE includes two cryptographic modules that provide cryptographic support for the VPN services. The cryptographic modules have been FIPS 140-2 validated on another platform (cert. #1991 and cert. #2013). The FIPS 140-2 validation addresses the detailed workings of the cryptographic functionality and provides the assurance that only secure key values are accepted for the applicable algorithms.

The cryptographic support provided by the TOE is defined in the security functional requirements:

- Cryptographic Operations

IPsec				
	Service	**Method**	**Standard**	**SFR**
ESP	Authentication and encryption	AES-GCM-128 AES-GCM-256	AES: FIPS 197 GCM mode: NIST SP 800-38D	FCS_COP.1a {Firewall/VPN} (FCS_IPSEC_EXT.1.4 {Firewall/VPN})
IKE v1, IKE v2				
	Service	**Method**	**Standard**	**SFR**
Messages (payload)	encryption	AES-CBC-128 AES-CBC-256	AES: FIPS 197 CBC mode: NIST SP 800-38A	FCS_COP.1a {Firewall/VPN} (FCS_IPSEC_EXT.1.6 {Firewall/VPN})
Messages (payload)	authentication	HMAC-SHA-256 HMAC-SHA-384	HMAC: FIPS 198-1	FCS_COP.1d {Firewall/VPN}
Peer authentication	Signature services (RSA, ECDSA)	RSA ECDSA	RSA: FIPS 186-3, PKCS #1 v2.1 (RSASSA-PKCSI-v1_5 scheme) ECDSA: FIPS 186-3	FCS_COP.1b {Firewall/VPN}
Peer authentication	Hash for signatures	SHA-256 SHA-384	SHA: FIPS 180-3	FCS_COP.1c {Firewall/VPN}

Table 11 Cryptographic Operations

- Cryptographic Keys

Key	Used for	Key size	Key generation standard	SFR
HMAC-SHA-256 HMAC-SHA-384	Symmetric key generation	256	NIST SP 800-56A, RFC 2409, RFC 5996	FCS_CKM.1c {Firewall/VPN}, FCS_RBG_EXT.1 {Firewall/VPN}
AES-GCM-128 AES-GCM-256 AES-CBC-128 AES-CBC-256	Symmetric key generation	128 and 256	FIPS 197, NIST SP 800-56A, RFC 2409, RFC 5996	FCS_CKM.1c {Firewall/VPN}, FCS_RBG_EXT.1 {Firewall/VPN}
ECDSA (IKE)	Signature keys for authentication	256 and 384 (P-256 and P-384)	FIPS 186-3 Appendix B.4.1	FCS_CKM.1b {Firewall/VPN}, FCS_RBG_EXT.1 {Firewall/VPN}
RSA (IKE)	Signature keys for authentication	2048	FIPS 186-3 Appendix B.3.6	FCS_CKM.1b {Firewall/VPN}, FCS_RBG_EXT.1 {Firewall/VPN}
DSA (IKE)	Key establishment keys	2048	FIPS 186-3 Appendix B.1.1	FCS_CKM.1a {Firewall/VPN}, FCS_RBG_EXT.1 {Firewall/VPN}
ECDSA (IKE)	Key establishment keys	256 and 384 (P-256 and P-384)	FIPS 186-3 Appendix B.4.1	FCS_CKM.1a {Firewall/VPN}, FCS_RBG_EXT.1 {Firewall/VPN}

Table 12 Cryptographic keys

- Cryptographic Key Destruction by zeroization

This TSF is mapped to the following SFRs: FCS_CKM.1a {Firewall/VPN}, FCS_CKM.1b {Firewall/VPN}, FCS_CKM.1c {Firewall/VPN}, FCS_CKM.4 {Firewall/VPN}, FCS_COP.1a {Firewall/VPN}, FCS_COP.1b {Firewall/VPN}, FCS_COP.1c {Firewall/VPN}, FCS_COP.1d {Firewall/VPN}, FCS_IPSEC_EXT.1 {Firewall/VPN}, FCS_RBG_EXT.1 {Firewall/VPN}.

7.3.5 VPN User Data Protection

The VPN service includes the creation of encrypted communication channels and the definition of encryption policies. Either the TOE or the peer security gateway can initiate the process to establish a VPN channel. It operates in a tunnel mode among the gateways using the IPSec protocol set as defined in RFC 4301 to integrate the following security functions:

- Authentication: public key exchanges and certificates protect the identity of communicating parties (see Identification and authentication below).
- Access control: VPN access is restricted by the firewall traffic filter and rule bases (see Information flow control above).
- Confidentiality: encryption methods protect data from unauthorized parties
- Data integrity: digital signatures ensure that unauthorized attempts to tamper with data cannot go unnoticed.

The IPsec protocol suite specifies the use of encryption to provide authentication, integrity and confidentiality security services. The TOE uses the Encapsulating Security Payload (ESP) protocol to provide confidentiality, data origin authentication, and connectionless integrity as described in Table 11 Cryptographic Operations.

The gateways negotiate to establish tunnels – two unidirectional connections called Security Associations (SAs) used to securely transmit data. SAs provide the information required to support the VPN connection, keys, algorithms, modes, and lifetimes. The SAs are negotiated using the Internet Key Exchange (IKE) as described in Table 11 Cryptographic Operations.

Two versions of IKE are available:

- IKE version 1 (IKEv1) as defined in RFC 2409
- IKE version 2 (IKEv2) as defined in RFC 5996

IKEv1 negotiation consists of two separate phases, IKE Phase 1 and IKE Phase 2. In IKEv2 there are IKE_SA and CHILD_SA negotiations.

During IKEv1 Phase 1 and IKEv2 IKE_SA negotiations the gateways authenticate each other and create an IKE SA, a secure channel for further negotiations (IKEv1 Phase 2 and IKEv2 child SAs). Authentication is done using a certificate based public key method (RSA or ECDSA signature and verification). Encryption keys are generated and exchanged using the DH or ECDH key agreement method for encryption during the IKE negotiation.

IKEv1 Phase 2 and IKEv2 CHILD_SA negotiations establish the encryption/decryption procedures for protecting the IP data traffic between the gateways. It generates a pair of SAs, which contains information for protecting the IP traffic. The negotiation of IPsec SAs is encrypted using the keys already agreed in the IKE SAs. The generated IPsec tunnels are used for conveying securely the actual data traffic between security gateways. The SA specified for IPsec sets the lifetime of the IPsec SAs.

This TSF is mapped to the following SFR: FCS_CKM.1a {Firewall/VPN}, FCS_CKM.1b {Firewall/VPN}, FCS_CKM.1c {Firewall/VPN}, FCS_CKM.4 {Firewall/VPN}, FCS_COP.1a {Firewall/VPN}, FCS_COP.1b {Firewall/VPN}, FCS_COP.1c {Firewall/VPN}, FCS_COP.1d {Firewall/VPN}, FCS_IPSEC_EXT.1 {Firewall/VPN}, FCS_RBG_EXT.1 {Firewall/VPN}.

7.3.5.1 VPN Policy Parameters

The security associations generated for the IKE and IPsec SAs broadly represent the encryption policy to be implemented. To add granularity to the encryption policy, authorized firewall administrators can specify the negotiation degree of security associations; Security Associations can be negotiated for each pair of communicating networks and hosts.

Symmetric Encryption Parameters: Symmetric encryption is used to provide confidentiality of data during the SA negotiation based on IKE proposals and is used for encrypting/decrypting IPSec payload data. The following symmetric algorithms can be specified:

- AES-GCM (IPsec payload encryption/decryption and authentication)
- AES-CBC (IKE message encryption/decryption)
- (3DES is included in the product for interoperability but is not included in the evaluation.)

Data Integrity Parameters: The HMAC-SHA keyed hash function is used to ensure the integrity of IKE messages exchanged.

Authentication Parameters: Certificate based public key methods are used to authenticate the gateways to each other. The following algorithms can be specified for gateway authentication:

- RSA signature
- ECDSA signature

Key Agreement Parameters: The following two parameters can be set for computing DH and ECDH values in the IKE negotiation mode and the IPsec mode:

- DH and ECDH group for IKE
- DH and ECDH group for Perfect Forward Secrecy (PFS)

Lifetime Parameters: The lifetime of the IKE can be specified in terms of elapsed time. The lifetime of the IPsec tunnels can be specified in terms of elapsed time and transferred data. Lifetime (minutes or KB) represents the overall time (or data volume) after which the opened tunnels are closed. If a new tunnel is needed, a re-negotiation process is started in IKEv2 while in IKEv1 the negotiation process is started over again. When an IPsec tunnel expires, IKEv1 Phase 2 or IKEv2 CHILD_SA negotiation is performed again based on the settings of the IPsec proposal and through the IKE negotiated tunnel. This process generates new key material to be used for the IPsec traffic. Similarly, IKE SAs are set to expire, but their lifetime is typically much longer than that of the IPsec SA since IKE SA negotiation is more complex.

This TSF is mapped to the following SFR: FCS_CKM.1a {Firewall/VPN}, FCS_CKM.1b {Firewall/VPN}, FCS_CKM.1c {Firewall/VPN}, FCS_CKM.4 {Firewall/VPN}, FCS_COP.1a {Firewall/VPN}, FCS_COP.1b {Firewall/VPN}, FCS_COP.1c {Firewall/VPN}, FCS_COP.1d {Firewall/VPN}, FCS_IPSEC_EXT.1 {Firewall/VPN}, FCS_RBG_EXT.1 {Firewall/VPN}.

7.3.6 Identification and authentication

The TOE provides the following Identification and Authentication mechanisms for other security gateways to establish a VPN connection with the TOE:

- Certificate-based using RSA digital signatures
- Certificate-based using ECDSA digital signatures

Other security gateways and the TOE authenticate each other when establishing a VPN connection, i.e., tunnel. This is done during the IKE SA negotiation of the IKE protocol. The certificate-based authentication method options are RSA and ECDSA signatures. Either side can initiate the connection, and based on the configuration setting, the appropriate authentication method is used. The cryptographic module within the TOE performs the required cryptographic operations.

The trust is established by using the RSA key pairs that have been generated by the TOE. The public key part is turned into certificates and signed by the SMC (part of the TOE environment and therefore outside of the scope of this ST).

This TSF is mapped to the following SFR: FCS_CKM.1b {Firewall/VPN}, FCS_COP.1b {Firewall/VPN}, FCS_COP.1c {Firewall/VPN}, FCS_IPSEC_EXT.1 {Firewall/VPN}.

7.4 INTRUSION DETECTION AND PREVENTION

The TSFs described in this section are only available to the TOE in the IPS role.

The Stonesoft IPS analyzes data as a normalized stream rather than as single or combined packets. The data stream is fed through multiple parallel and sequential state machines for deep inspection.

In the IP and TCP protocol layers on OSI model, the Stonesoft IPS makes sure that there is a unique way to reconstruct the data stream. The Stonesoft IPS passes through well-formed IP fragments and TCP segments with minimum or no modification. Fragments or segments with conflicting and overlapping data are dropped. This normalization process determines that there is a unique way to interpret the network traffic passing through the IPS. The actual data stream is reassembled for inspection in the upper protocol layers.

In the Session and Application protocol layers, Stonesoft can identify certain protocol and application elements in the data stream and, when appropriate, inspect them as separate data streams that can be normalized depending on the protocol context.

In the Application layer, both vulnerability and attack-based signatures are used for detecting exploits in the normalized application data stream.

Signatures are based on regular expression language. Regular expressions match byte sequences in application data stream. The regular expression consists of one or more branches. The signature matches if any of the branches matches to the byte stream.

7.4.1 Information flow control

The information flow control is performed in the following four steps:

1. The engine checks Ethernet frames against the Ethernet rules in the policy. The packet is processed until it matches an Ethernet rule that tells whether to allow or to discard the packet.
2. The engine checks the current connection tracking information to see if the packet is part of an established connection (for example, a reply packet to a request that has been allowed).
3. If the packet is not part of an existing connection, the packet is matched to the IPv4 Access rules according to the IP protocol used.
    - The processing of the packet continues until the packet matches a rule that tells the engine to allow or discard the packet. If the packet does not match any Access rule, the final action depends on the engine type. An IPS engine allows the packet to pass through.
4. The engine matches connections that are selected for deep packet inspection in the IPv4 Access rules against the Inspection rules. Note that only IPv4 is part of the evaluated configuration and not IPv6.
    - The Inspection rules are used to look for patterns of interest in allowed connections. The patterns may indicate potential attacks, exploits, or other possible threats. Alternatively, they can be any other patterns that might be of interest, such as multiple login attempts, use of peer-to-peer or instant messaging software, or protocol violations in the traffic.

- If a pattern in traffic matches a pattern defined in a rule, the action(s) defined in the rule are taken.

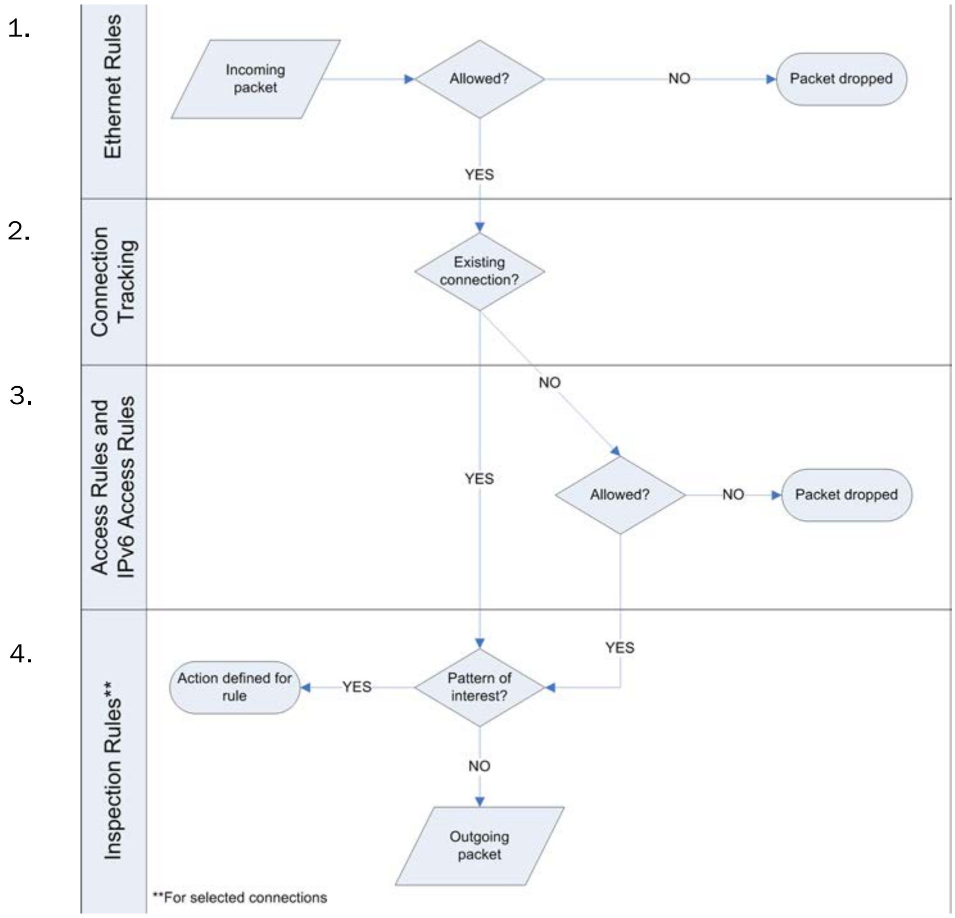

Figure 4, Packet/Connection Handling in an inline IPS.

Packets that are dropped by the information flow control are either silently discarded or refused.

This TSF is mapped to the following SFRs: FDP_IFC.2 {IPS}, FDP_IFF.1 {IPS}

ANNEX A ACRONYMS

3DES	Triple DES (Data Encryption Standard)
AES	Advanced Encryption Standard
CA	Certificate Authorities
CBC	Cipher Block Chaining
CC	Common Criteria for IT Security Evaluation
CM	Configuration Management
CVI	Cluster Virtual interface
EAL	Evaluation Assurance Level
ESP	Encapsulating Security Payload
FIPS	Federal Information processing Standard
FTP	File Transfer Protocol
GUI	Graphical User Interface
GNU	GNU’s Not Unix (recursive)
HMAC	Hash Message Authentication Code
HTTP	Hyper Text Transfer Protocol
ICMP	Internet Control Message Protocol
IKE	Internet Key Exchange
IPsec	Internet Protocol Security
LDAP	Lightweight Directory Access Protocol
NAT	Network Address Translation
NIAP	National Information Assurance Partnership
NIC	Network interface Card
NDI	Node Detected Interface
PFS	Perfect Forward Secrecy
PKCS	Public Key Cryptography Standards
RFC	Request For Comments
RSA	Rivest, Shamir and Adleman
SF	Security Function
SHA	Secure Hashing Algorithm
SFP	Security Function Policy
SGW	Security Gateway
SMTP	Simple Mail Transfer Protocol
SSH	Secure Shell
SSL	Secure Socket Layer
ST	Security Target
TCP	Transmission Control Protocol
TLS	Transport Layer Security
TOE	Target of Evaluation
TSC	TSF Scope of Control
TSF	TOE Security Functions

TSP	TOE Security Policy
UDP	User Datagram Protocol
VAR	Value-Added Reseller
VPN	Virtual Private Network
VPNC	VPN Consortium

ANNEX B TERMINOLOGY

Certificate, Digital
An electronic identification card for a user or device. Digital certificates are distributed, or granted, by certificate authorities (CAs), and ensure that the user or device is who/what they claim to be. Digital certificate holders have a public and private key pair, which can be used to sign messages (authenticate the sender), and decrypt incoming messages (ensuring only the certificate holder can decode the encrypted message).

Clustering Technology
A set of methods and algorithms used to implement highly scalable solutions where more than one machine handles the work load. The advantages of clustering technology include increased performance, availability, and reliability.

Connection Tracking
The set of data maintained for a connection. Used for relating incoming packets to existing connections. Connection tracking also includes information to support features like NAT, Load Balanced Routing and Protocol Agents. May also contain accounting information.

Firewall
A barrier or choke point between two or more networks, which examines, controls and/or blocks the flow of data between those networks. Often thought of as a defense between a corporate network and the Internet, firewalls can also protect internal networks from each other.

Firewall Cluster
A group of firewalls that, through clustering technology, process the work normally performed by a single firewall machine.

Firewall Engine
The application software or processes that run on a firewall, performing the actual examination and access control of data.

Firewall Node
A single device, often a specialized PC or router, which runs firewall software, and performs the functions of a firewall as part of a firewall cluster.

Firewall Security Policy
A rule base that defines the policies implemented by the firewall for securing network and computer resources.

Firewall System
A collection of applications used to implement security policies and monitor network traffic at one or more sites. A firewall system consists of firewall engines, Management Servers, Log Servers and GUIs.

High Availability
The implementation of clustering technology, hot standby technology, or general redundancy in a system to increase the availability of an application, service, or network beyond what a single system is capable of providing. Increased availability is achieved by eliminating all single points of failure, with clustering technology providing the highest level of availability.

Multi-Layer Inspection
A hybrid firewall technology that incorporates the best elements of application-level and network-level firewalls, with additional technology to enable the secure handling of many connection types.

NAT (Network Address Translation)
A mechanism for assigning local networks a set of IP addresses for internal traffic and another for external traffic. NAT was originally described in RFC 1631 as a means for solving the rapidly diminishing IP address space. It provides a supplemental security purpose by hiding internal IP addresses.

Packet
A unit of data sent across a network.

Packet Filtering
A method of controlling access to a network, or set of networks, by examining packets for source and destination address information, and permitting those packets to pass, or halting them based on defined rules.

Protocol

An agreed-upon format for transmitting data between two or more devices. Protocols typically define how to check for errors, how the sender will announce they have completed the sending of data, how the receiver will acknowledge receipt of the data, and how they will compress the data (if applicable).

Protocol Agent
A module that assists the firewall engine in handling a particular protocol. Protocol agents ensure that related connections for a service are properly grouped and evaluated by the firewall engine, as well as assisting the engine with content filtering or network address translation tasks.

Route
The set of routers or gateways a packet travels through in order to reach its destination. In TCP/IP networks, individual packets for a connection may travel through different routes to reach the destination host.

ANNEX C REFERENCES

Stonesoft Documentation

[1] Stonesoft Firewall/VPN Installation Guide, Version 5.5, Revision SGFIG_20130624.

[2] Stonesoft Firewall/VPN Reference Guide, Version 5.5, Revision SGFRG_20131126.

[3] Stonesoft IPS and Layer 2 Installation Guide, Version 5.5, Revision SGIIG_20130618.

[4] Stonesoft IPS and Layer 2 Reference Guide, Version 5.5, Revision SGIRG_20130624.

[5] Stonesoft Administrator's Guide, Version 5.5, Revision SGAG_20131202.

[6] Common Criteria Certification User's Guide, Version 5.5, Revision SGCC_20140417.

Standards

[CC] Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 4, September 2012.

[NIAP-0414] NIAP Interpretation 0414, Site-configurable prevention of audit loss, Effective date 4 January 2002.

[NDPP] Network Device Protection Profile (NDPP), Version 1.1, 08 June 2012

[NDPP-VPN] Network Device Protection Profile (NDPP) Extended Package VPN Gateway, Version 1.1, 12 April 2013

[PKCS1v2.1] PKCS #1 v2.1: RSA Cryptography Standard, RSA Laboratories, 14. June 2002

[RFC1631] RFC 1631 - The IP Network Address Translator (NAT), May 1994

[RFC2407] RFC 2407 - The Internet IP Security Domain of Interpretation for ISAKMP, November 1998

[RFC2408] RFC 2408 - Internet Security Association and Key Management Protocol (ISAKMP), November 1998

[RFC2409] RFC 2409 - The Internet Key Exchange (IKE), November 1998

[RFC4301] RFC 4301 - Security Architecture for the Internet Protocol, December 2005

[RFC4303] RFC 4303 - IP Encapsulating Security Payload (ESP), December 2005

[RFC4106] RFC 4106 - The Use of Galois/Counter Mode (GCM) in IPsec Encapsulating Security Payload (ESP), June 2005

[RFC4109] RFC 4109 - Algorithms for Internet Key Exchange version 1 (IKEv1), May 2005

[RFC4868] RFC 4868 - Using HMAC-SHA-256, HMAC-SHA-384, and HMAC-SHA-512 with IPsec, May 2007

[RFC4945] RFC 4945 - The Internet IP Security PKI Profile of IKEv1/ISAKMP, IKEv2, and PKIX, August 2007

[RFC5996] RFC 5996 - Internet Key Exchange Protocol Version 2 (IKEv2), September 2010

[RFC6379] RFC 6379 - Suite B Cryptographic Suites for IPsec, October 2011

[FIPS140] NIST FIPS PUB 140–2 – Security Requirements for Cryptographic Modules, December 3, 2002

[FIPS197] NIST FIPS PUB 197 – Specification for the Advanced Encryption Standard (AES), November 26, 2001

[NIST800-90A] NIST Special Publication 800-90A - Recommendation for Random Number Generation Using Deterministic Random Bit Generators, January 2012

ANNEX D NETWORK INTERFACE CARDS

The following network interface cards are available with appliances that are within the scope of the evaluation:

MIL-320

4 x 10/100/1000 Mbit/s Intel 82583V ports

Wi-Fi Atheros AR9280

1035

4 x 10/100/1000 Mbit/s Intel I347-T4

In addition to that there is one PCI Express expansion slot for modules presented in the table below.

1065

4 x 10/100/1000 Mbit/s Intel I347-T4

In addition to that there is one PCI Express expansion slot for modules presented in the table below.

1405

4 x 10/100/1000 Mbit/s Intel I350-AM4

In addition to that there is one PCI Express expansion slot for modules presented in the table below.

3202

2 x 10/100/1000 Mbit/s Intel 82574L ports onboard

In addition to that there are three PCI Express expansions slots for modules presented in the table below.

3206

2 x 10/100/1000 Mbit/s Intel I350 ports onboard

In addition to that there are three PCI Express expansions slots for modules presented in the table below.

5206

2 x 10/100/1000 Mbit/s Intel I350 ports onboard

In addition to that there are six PCI Express expansions slots for modules presented in the table below.

Module	Ports	Code
GE8	8 x 10/100/1000 Mbit/s Intel 82576EB	MOD-EM1-GE-8
GESFP4	4 x SFP transceiver openings for SFP transceivers presented in the table below	MOD-EM1-GE-SFP-4
10GSFP2	2 x SFP+ transceiver openings for SFP+ transceivers presented in the table below	MOD-EM1-10G-SFP-2

Transceiver	Port	Code
TX SFP	10/100/1000 Mbit/s copper	MOD-SFP-GE-TX
SX SFP	1000 Mbit/s multi-mode fiber	MOD-SFP-GE-SX
LX10 SFP	1000 Mbit/s single-mode fiber	MOD-SFP-GE-LX10
SR SFP+	10 Gbit/s multi-mode fiber	MOD-SFP-10G-SR
LR SFP+	10 Gbit/s single-mode fiber	MOD-SFP-10G-LR