SonicWALL, Inc.
SonicOS v5.0.1 on NSA Series and TZ Series Appliances

Security Target

Evaluation Assurance Level: EAL 4+
Document Version: 0.7

Prepared for:

SonicWALL, Inc.
1143 Borregas Avenue
Sunnyvale, CA 94089-1306
USA
Phone: (888) 557-6642

http://www.sonicwall.com

Prepared by:

Corsec Security, Inc.
10340 Democracy Lane, Suite 201
Fairfax, VA 22030
USA
Phone: (703) 267-6050

http://www.corsec.com

Revision History

Version	Modification Date	Modified By	Description of Changes
0.1	2007-06-06	Amy Nicewick	Initial draft.
0.2	2007-06-22	Amy Nicewick	Name change.
0.3	2007-07-31	Amy Nicewick	Modifications related to cryptography claims.
0.4	2007-12-12	Greg Milliken	Updates for ASE-DES-CR-2.
0.5	2008-01-30	Amy Nicewick	Addressed verdicts for SPM.
0.6	2008-04-24	Greg Milliken	Addressed verdicts from CB-ASE-OR1 and PETR v1.2 Updated crypto tables according to customer requested changes. Updated assurance requirements table with list of installation guides.
0.7	2008-04-28	Greg Milliken	Reworded the rationale for FDP_ITC.1.

Table of Contents

Table of Figures

Table of Tables

1 Security Target Introduction

This section identifies the Security Target (ST), Target of Evaluation (TOE), ST conventions, ST conformance claims, and the ST organization. The Target of Evaluation is the SonicWALL SonicOS v5.0.1 on NSA Series and TZ Series Appliances, and will hereafter be referred to as the TOE throughout this document. The TOE is a unified threat management (UTM) device.

1.1 Purpose

This ST provides mapping of the Security Environment to the Security Requirements that the TOE meets in order to remove, diminish or mitigate the defined threats in the following sections:

- Security Target Introduction (Section 1) – Provides a brief summary of the ST contents and describes the organization of other sections within this document.
- TOE Description (Section 2) – Provides an overview of the TOE security functions and describes the physical and logical boundaries for the TOE.
- Security Environment (Section 3) – Describes the threats and assumptions that pertain to the TOE and its environment.
- Security Objectives (Section 4) – Identifies the security objectives that are satisfied by the TOE and its environment.
- Security Requirements (Section 5) – Presents the Security Functional Requirements (SFRs) and Security Assurance Requirements (SARs) met by the TOE and by the TOE's environment.
- TOE Summary Specification (Section 6) – Describes the security functions provided by the TOE that satisfy the security functional requirements and objectives.
- Protection Profile Claims (Section 7) – Provides the identification of any ST Protection Profile claims as well as a justification to support such claims.
- Rationale (Section 8) – Presents the rationale for the security objectives, requirements, and the TOE summary specifications that relate to their consistency, completeness, and suitability.
- Acronyms (Section 9) – Defines the acronyms used within this ST.

1.2 Security Target, TOE and CC Identification and Conformance

Table 1 - ST, TOE, and CC Identification and Conformance

ST Title	SonicWALL, Inc. SonicOS v5.0.1 on NSA Series and TZ Series Appliances Security Target
ST Version	Version 0.7
Author	Corsec Security, Inc. Amy Nicewick and Matt Keller
TOE Identification	SonicWALL SonicOS v5.0.1 on NSA Series and TZ Series Appliances
Common Criteria (CC) Identification and Conformance	Common Criteria for Information Technology Security Evaluation, Version 2.3, [August 2005] (aligned with ISO/IEC 15408:2005); CC Part 2 extended; CC Part 3 augmented; PP claim (none); Parts 2 and 3 Interpretations from the Interpreted CEM as of 2007/07/11 were reviewed, and no interpretations apply to the claims made in this ST.
Protection Profile (PP) Identification	None
Evaluation Assurance Level	EAL 4+ (Augmented with ALC_FLR.1)
Keywords	Firewall, VPN, Information Flow Control

1.3 Conventions, Acronyms, and Terminology

1.3.1 Conventions

There are several font variations used within this ST. Selected presentation choices are discussed here to aid the ST reader.

The Common Criteria for Information Technology Security Evaluation (CC) allows for assignment, refinement, selection and iteration operations to be performed on security functional requirements. All of these operations are used within this ST. These operations are performed as described in Parts 2 and 3 of the CC, and are shown as follows:

- Completed assignment statements are identified using [*italicized text within brackets*].
- Completed selection statements are identified using [<u>*underlined italicized text within brackets*</u>].
- Refinements are identified using **bold text**. Any text removed is stricken (Example: ~~TSF Data~~) and should be considered as a refinement.
- Iterations are identified by appending a letter in parentheses following the component title. For example, FAU_GEN.1(a) Audit Data Generation would be the first iteration and FAU_GEN.1(b) Audit Data Generation would be the second iteration.
- Explicitly stated requirements are followed by the text (EXP).

1.3.2 Acronyms

The acronyms used within this ST are described in Section 9 – “Acronyms.”

1.3.3 Terminology

The term “User” is defined in this document as an individual or IT entity passing information through the TOE.

The term “Administrator” is defined in this document as an individual authorized to perform management functions on the TOE.

2 TOE Description

The TOE Description provides an overview of the TOE. This section describes the general capabilities and security functionality of the TOE. The TOE description provides context for the TOE evaluation by identifying the product type, describing the product, and defining the specific evaluated configuration. The TOE is designed and manufactured by SonicWALL, Incorporated, hereafter referred to as SonicWALL, in Sunnyvale, California.

2.1 Product Type

SonicWALL SonicOS v5.0.1 on NSA Series and TZ Series Appliances is custom software running on purpose built hardware platforms that combine to form a UTM device. UTMs are network firewalls that provide additional features, such as spam filtering, anti-virus capabilities, intrusion prevention systems (IPS), and World Wide Web content filtering[1]. The product under evaluation consists of the SonicOS Enhanced operating system for the following appliances: TZ180, TZ180W, TZ190, TZ190W, NSA 3500, NSA 4500, NSA 5000, NSA E5500, NSA E6500, and NSA E7500. All appliances share similar physical specifications, varying only in available features, processor cores, speed, and memory. These appliances provide firewall, UTM, Virtual Private Networking (VPN), and traffic management capabilities. The product is managed using a web-based Graphical User Interface (GUI) accessed through a permitted device running a supported web browser connected directly to the appliance over a network cable and communicating via HTTPS.

Figure 1 below shows a possible deployment configuration of the product, showing its placement within a network:

[1] Please note that the spam filtering and World Wide Web content filtering functionality is not included as a part of this evaluation.

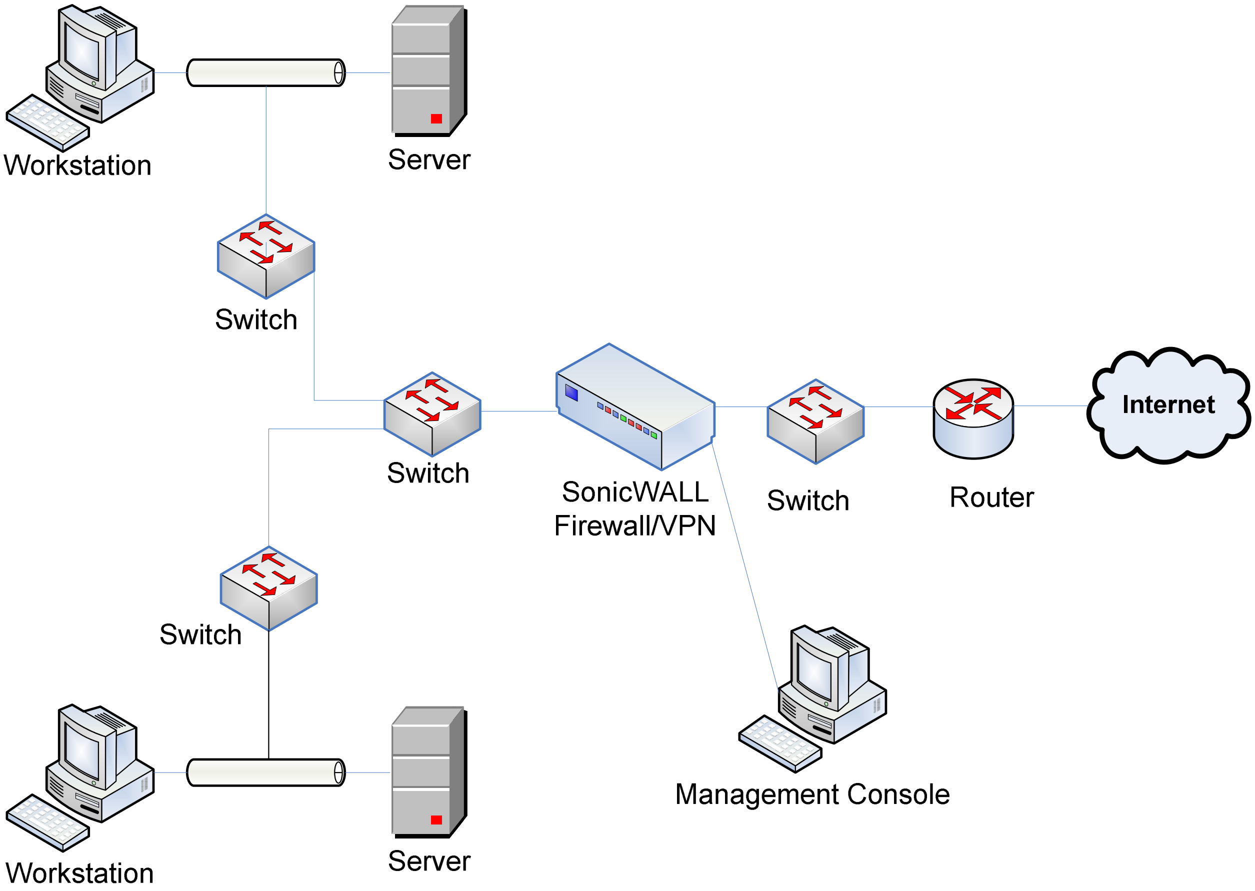

Figure 1 - Deployment Configuration of the TOE

2.2 Product Description

The SonicOS Enhanced is a proprietary operating system designed for use on SonicWALL appliances. The evaluated appliances run only signed SonicOS firmware, and are licensed to provide a selection of features to the end user. SonicOS provides policy-based network traffic control, UTM, and VPN services.

SonicOS's firewall capabilities include stateful packet inspection. Stateful packet inspection keeps track of the state of network connections, such as Transmission Control Protocol (TCP) streams and User Datagram Protocol (UDP) communication, traveling across the firewall. The firewall distinguishes between legitimate packets and illegitimate packets for the given network deployment. Only packets adhering to the administrator-configured access rules are allowed to pass through the firewall; all others are rejected.

SonicOS's UTM capabilities include deep-packet inspection (DPI). The optional licensed services that make up the UTM include IPS, Gateway Anti Virus (GAV), and Gateway Anti-Spyware (SPY). All UTM services employ stream-based analysis wherein traffic traversing the product is parsed and interpreted so that its content might be matched against sets of signatures to determine the acceptability of the traffic. The parsing and interpretation engines allow for the reliable handling of various protocols (such as Simple Mail Transfer Protocol (SMTP), Hypertext Transfer Protocol (HTTP), File Transfer Protocol (FTP), Post Office Protocol (POP), Internet Message Access Protocol (IMAP), as well as Generic TCP), encodings (Multipurpose Internet Mail Extensions (MIME), Base64, Unix-to-Unix Encode (UUEncode)), and types of compression (Compressed File (ZIP), Gnu Compressed File (GZIP), Lempel-Ziv Coding 1977 (LZ77)). In the event a certain flow of traffic is found to match an

IPS/GAV/SPY signature meeting or exceeding the configured threshold, the event is logged, and the offending flow is terminated.

SonicOS supports VPN functionality[2], which provides a secure connection between two or more computers or protected networks over the public internet. It provides authentication to ensure that the information is going to and from the correct parties, and protects the information from viewing or tampering en route. SonicOS supports the creation and management of Internet Protocol Security (IPSec) VPNs. IPSec is a suite of protocols that operate on network traffic to secure Internet Protocol (IP) communications by authenticating and encrypting packets. Cryptographic key establishment is also possible through IPSec. For this, SonicOS supports Internet Key Exchange (IKE), which is the protocol used to set up a security association (SA) in the IPSec protocol suite. SonicOS enables VPN policy creation to provide the configuration of multiple VPN tunnels. VPN policy definitions include the IP address of the remote gateway appliance with which the product will communicate, the IP address of the destination network, the type of encryption used for the policy, and other configuration information.

SonicOS provides site-to-site VPN functionality. Site-to-site VPN functionality allows creation of VPN policies for connecting offices running SonicWALL security appliances, resulting in network-to-network VPN connections.

Digital certificates are also supported by SonicOS. A digital certificate is an electronic means to verify identity by a trusted third party known as a Certification Authority (CA). SonicOS users can obtain certificates signed and verified by a third party CA to use with an IKE VPN policy. This makes it possible for VPN users to authenticate peer devices without manually exchanging shared secrets or symmetric keys. SonicOS interoperates with any X.509v3-compliant provider of certificates.

The product implements both physical and virtual interfaces. Physical interfaces are bound to a single port. Virtual interfaces are assigned as sub-interfaces to a physical interface, and allow the physical interface to carry traffic assigned to multiple virtual interfaces. The product allows static IP address configuration on all physical and logical network interfaces, as well as dynamic configuration of WAN interfaces through Dynamic Host Configuration Protocol (DHCP), Point to Point over Ethernet (PPPoE) Point to Point Tunneling Protocol (PPTP), and Layer 2 Tunneling Protocol (L2TP). Additionally, interface pairs may be configured in a Layer 2 (L2) Bridge mode to enable the inspection and control of traffic between the resulting two segments without a need for logical reconfiguration of the target network.

In addition, physical interfaces may be assigned to Security Zones. Zones are optional logical groupings of one or more interfaces designed to make management of the product simpler and to allow for configuration of access rules governing inbound and outbound traffic. If there is no interface, traffic cannot access the zone or exit the zone. Zones allow the administrator to group similar interfaces and apply the same policies to them, instead of having to write the same policy for each interface. In this way, access to critical internal resources such as payroll servers or engineering code servers can be strictly controlled. Zones may be one of several types: Trusted (e.g., Local Area Network (LAN)), Untrusted (e.g., WAN), Public (e.g., Demilitarized Zone (DMZ)), Encrypted (e.g., VPN), and Wireless, as well as custom zones.

- Trusted zones provide the highest level of trust. In other words, the least amount of scrutiny is applied to traffic coming from trusted zones. The LAN zone is always trusted. Conversely, traffic destined to a trusted zone is subject to the greatest scrutiny.
- Untrusted zones represent the lowest level of trust. Traffic from untrusted zones is not permitted to enter any other zone type without explicit rules, but traffic from any other zone type is permitted to enter Untrusted zones.
- Public zones offer a higher level of trust than Untrusted zones, but a lower level of trust than Trusted zones. Traffic from a Public zone to a trusted zone is denied by default. But traffic from any Trusted zone to any other zone is allowed.

[2] For use with SonicWALL Global VPN Client. Global VPN Client is another SonicWALL product that is not a part of this evaluation.

- Encrypted zones are used exclusively by the VPN functionality of SonicOS. All traffic to and from an Encrypted zone is encrypted.
- Wireless zones are zones where the only interface to the network consists of SonicWALL SonicPoint (wireless) devices. Wireless zones are not part of the evaluated configuration of the product.

SonicOS also provides client functionality for Domain Name System (DNS) resolution, Address Resolution Protocol (ARP), and Network Address Translation (NAT). It includes a Network Time Protocol (NTP) client that automatically adjusts the product's clock, which provides time stamps for log events, automatic updates to services, and other internal purposes.

An administrator manages SonicOS through a web GUI interface, using HTTP or Hypertext Transfer Protocol over SSL (HTTPS) and a web browser. All management activities can be performed through the Management Console, via a hierarchy of menu buttons. These activities include:

- viewing status of actions executed in the Management Console,
- managing licenses, certificates, SonicOS firmware, ARP traffic, and log events and settings,
- configuring administration settings, time settings, interfaces, zones, DNS settings, Address Objects, routes, NAT policies, firewall access rules, and VPN policies,
- setting schedules,
- using diagnostic tools,
- restarting the product, and
- setting up the DHCP server.

Event logging by SonicOS provides a mechanism for tracking potential security threats. Administrators can view and sort the log via the Management Console, configure the log events to be automatically sent to an e-mail address for alerting, convenience, or archiving, or export the logs to an Excel file or other application. Only authorized administrators can delete the contents of the log.

The product has three modes of operation: Central-site Gateway Mode (NAT and routing: this is the default for interfaces), Layer 2 Bridged Mode, and Transparent Mode. Multiple modes of operation can exist simultaneously, for example, if interface X1 is configured as a Primary Bridge Interface paired to interface X3 as a Secondary Bridge Interface, interface X1 can simultaneously operate in its traditional role as the Primary WAN, performing NAT for Internet-bound traffic through the Auto-added interface X1 Default NAT Policy.

Central-site Gateway Mode allows each interface to provide typical routing functionality. Transparent Mode allows a SonicWALL appliance to be introduced into a network without the need for re-addressing. Transport Mode presents an issue of temporarily disrupting certain protocols, such as ARP, Virtual LAN support, multiple subnets, and non-IP-version-4 traffic types. Layer 2 Bridged mode allows the SonicWALL device to be introduced onto the network without the need for re-addressing, but also addresses the issues presented by Transparent mode.

2.3 TOE Boundaries and Scope

This section addresses the physical and logical components of the TOE included in the evaluation.

2.3.1 Physical Boundary

Figure 2 illustrates the physical scope and the physical boundary of the SonicWALL SonicOS v5.0.1 on NSA Series and TZ Series Appliances, hereafter referred to as the TOE, and ties together the TOE and the constituents of the TOE Environment.

The TOE is a Firewall/UTM/VPN which runs on a TZ180 cluster (TZ180 and TZ180W), TZ190 cluster (TZ190 and TZ190W), NSA 3500/4500/5000 cluster, NSA E6500/E5500 cluster, or NSA E7500 SonicWALL appliance. The appliance is installed on a network wherever firewall/UTM/VPN services are required, as depicted in Figure 2 below. This may be used at the edge of a network for perimeter security or between different segments of a network for internal security. Please note that all functionality described in Section 2.2 is included in the CC evaluation, unless specifically listed in Section 2.3.3 - Physical/Logical Features and Functionality Not Included in the Evaluated Configuration of the TOE.

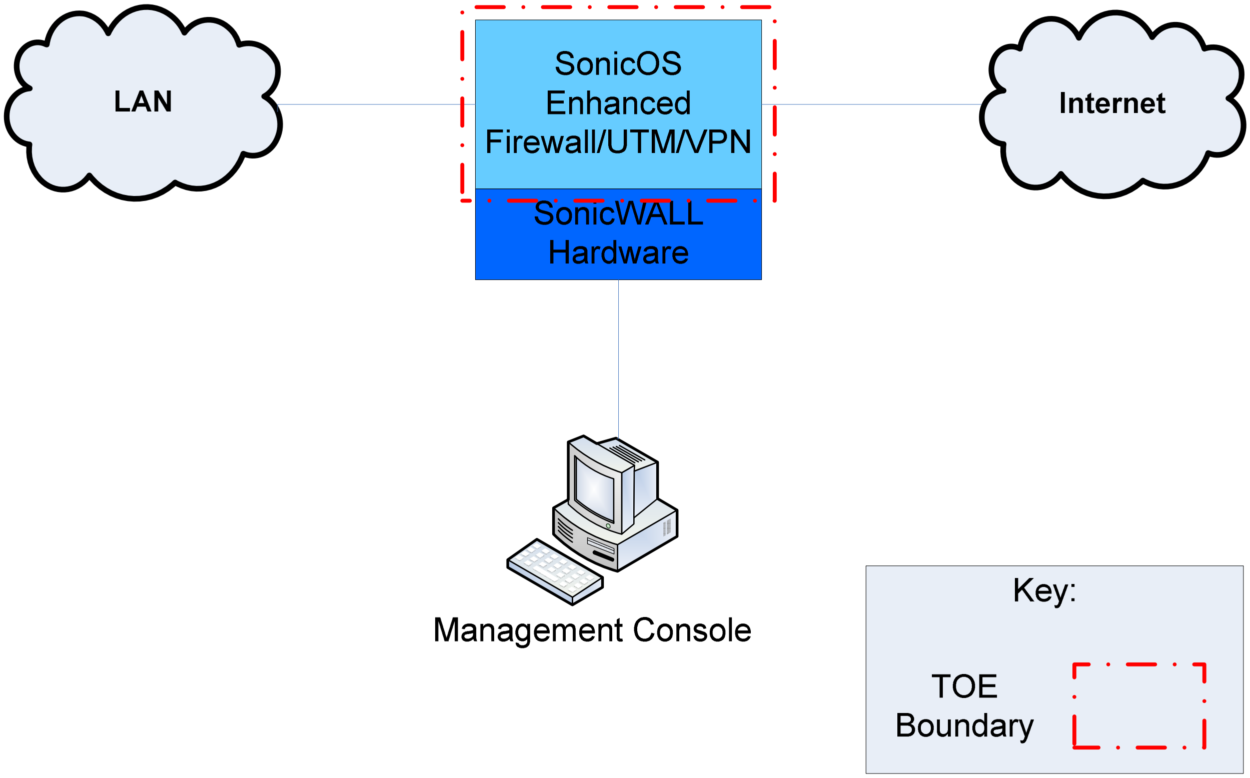

Figure 2 - Physical TOE Boundary

2.3.1.1 TOE Environment

The TOE environment consists of the SonicWALL hardware for the appliances listed above in Section 2.3.1, and the Management Console for managing the TOE. The hardware provides a timestamp to the TOE for auditing and scheduling. The environment also includes a hardware accelerator chip that can be used for speeding up encryption and decryption functions.

2.3.1.1.1 Security Considerations in the TOE Environment:

The Management Console must be locally connected to the TOE via a crossover cable. This is to ensure secure administration of the TOE without the possibility of traffic between the Management Console and the TOE being captured or traced.

2.3.2 Logical Boundary

The security functional requirements implemented by the TOE are usefully grouped under the following Security Function Classes:

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

- Security Management
- Protection of the TSF
- TOE Access

2.3.2.1 Security Audit

The Security Audit function provides the TOE with the functionality for generation, storage, and viewing of audit records. As administrators manage and configure the TOE, their activities are tracked by recording audit records into the logs. All security-relevant configuration settings and changes are recorded to ensure accountability of the administrator's actions. Activity by users is also recorded in the audit logs.

The TOE administrator has the ability to view all audit information from the audit logs, as well as search and sort the audit data. The TOE protects the stored audit records from unauthorized deletion and modification.

2.3.2.2 Cryptographic Support

The TOE provides IPSec VPN functionality for secure communications between two or more computers or protected networks over the public internet. This provides user authentication and encryption of information being passed through the VPN tunnel. Keys are generated and destroyed securely. All cryptographic operations are performed by a Federal Information Processing Standard (FIPS) 140-2 validated cryptographic module.

2.3.2.3 User Data Protection

The User Data Protection function implements functionality for TOE security functions and TOE security function policies related to protecting user data. The user data the TOE is protecting is the information passing through the TOE. This functionality is provided by the application of firewall access rules.

Note: The explicit Security Functional Policies are fully described in the Informal Security Policy Model document (*SonicWALL SonicOS v5.0.1 on NSA Series and TZ Series Appliances: Informal Security Policy Model*).

2.3.2.4 Identification and Authentication

The Identification and Authentication function provides functionality to establish and verify a claimed user identity. This ensures that the user has the appropriate privileges associated with the assigned role.

2.3.2.5 Security Management

The Security Management function specifies the management of several aspects of the TOE Security Function (TSF), including security function behavior and security attributes. The various management roles are also specified here.

2.3.2.6 Protection of the TSF

The Protection of the TSF function provides the integrity and management of the mechanisms that provide the TSF. The security functional requirements in this evaluation are impossible to bypass because the TOE is designed in such a way that no access is possible without passing through key security features. These features include identification, authentication, and information flow control mediation. The TOE is an operating system that maintains a security domain for its own execution.

2.3.2.7 TOE Access

The TOE Access function specifies requirements for controlling the establishment of a user's session. The TSF provides this function by terminating an interactive management session after a configurable time interval of administrator inactivity at the Management Console.

2.3.3 Physical/Logical Features and Functionality Not Included in the Evaluated Configuration of the TOE

The TOE is a software-only TOE[3]. Therefore the physical hardware is not included in the TOE boundary. Other features and functionality that are not part of the evaluated configuration of the TOE are:

- Command Line Interface (CLI) (Secure Shell, or SSH)
- Remote management and login (Remote Authentication Dial-In User Service (RADIUS), Lightweight Directory Access Protocol (LDAP), Active Directory, eDirectory authentication)
- NTP Server
- Application Firewall
- Web Content Filtering
- Hardware Failover
- Real-time Blacklist (SMTP)
- Global Security Client (including GroupVPN)
- Global Management System (GMS)
- SonicPoint

[3] The FIPS 140-2 validation lists the TOE as firmware. The firmware image file for SonicOS v5.0.1 as implemented on the custom NSA and TZ Series hardware is the software TOE as described in this document.

3 Security Environment

This section describes the security aspects of the environment in which the TOE will be used and the manner in which the TOE is expected to be employed. It provides the statement of the TOE security environment, which identifies and explains all:

- Assumptions about the secure usage of the TOE, including physical, personnel and connectivity aspects
- Known and presumed threats countered by either the TOE or by the security environment
- Organizational security policies with which the TOE must comply

3.1 Assumptions

Table 2 describes the security aspects of the intended environment for the evaluated TOE. The operational environment must be managed in accordance with assurance requirement documentation for delivery, operation, and user guidance. The following specific conditions are required to ensure the security of the TOE and are assumed to exist in an environment where this TOE is employed.

Table 2 - Assumptions

Name	Description
A.NOEVIL	Authorized administrators are non-hostile and follow all administrator guidance.
A.GENPUR	The TOE only stores and executes security-relevant applications and only stores data required for its secure operation.
A.DIRECT	The TOE is available to authorized administrators only.
A.PHYSEC	The TOE is physically secure.
A.MODEXP	The threat of malicious attacks aimed at discovering exploitable vulnerabilities is considered low.
A.PUBLIC	The TOE does not host public data.
A.SINGEN	Information cannot flow among the internal and external networks unless it passes through the TOE.

A.REMACC	Authorized administrators may only access the TOE locally.
A.UPS	The TOE will be supported by an Uninterruptible Power Supply.
A.AUDSTG	Prior to audit storage exhaustion on the TOE, the audit records will be exported either via SMTP or to an external Syslog server for persistent storage.
A.FIPS	The TOE will only be installed and run on SonicWALL appliances that have been validated to FIPS 140-2 with the same version of the TOE.

3.2 Threats to Security

This section identifies the threats to the IT assets against which protection is required by the TOE or by the security environment. The threat agents are divided into two categories:

- Attackers who are not TOE administrators: They have public knowledge of how the TOE operates and are assumed to possess a low skill level, limited resources to alter TOE configuration settings/parameters and no physical access to the TOE.
- TOE administrators: They have extensive knowledge of how the TOE operates and are assumed to possess a high skill level, moderate resources to alter TOE configuration settings/parameters and physical access to the TOE. (TOE administrators are, however, assumed not to be willfully hostile to the TOE.)

Both are assumed to have a low level of motivation. The IT assets requiring protection are the user data saved on or transitioning through the TOE and the hosts on the protected network. Removal, diminution and mitigation of the threats are through the objectives identified in Section 4 - Security Objectives.

The threats shown in Table 3 are applicable.

Table 3 - Threats

Name	Description
T.ASPOOF	An unauthorized entity may carry out spoofing in which information flows through the TOE into a connected network by using a spoofed source address.
T.AUDACC	Persons may not be accountable for the actions that they conduct, thus allowing an attacker to escape detection.

T.SELPRO	An unauthorized user may read, modify, or destroy security critical TOE configuration data stored on the TOE.
T.REPEAT	An unauthorized person may repeatedly try to guess authentication data used for performing I&A functionality in order to use this information to launch attacks on the TOE.
T.NOAUTH	An unauthorized user may attempt to bypass the security of the TOE so as to access and use security functions and/or non-security functions provided by the TOE.
T.MEDIAT	An unauthorized person may send impermissible information through the TOE which results in the exploitation of resources on the internal network.
T.AUDFUL	An unauthorized user may cause 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.NACCESS	An unauthorized person or external IT entity may be able to view data that is transmitted between the TOE and a remote authorized external IT entity.
T.NMODIFY	An unauthorized person or external IT entity may modify data that is transmitted between the TOE and a remote authorized external entity.

3.3 Organizational Security Policies

There are no Organizational Security Policies.

4 Security Objectives

This section identifies the security objectives for the TOE and its supporting environment. The security objectives identify the responsibilities of the TOE and its environment to meet the TOE's security needs.

4.1 Security Objectives for the TOE

The specific security objectives are shown in Table 4.

Table 4 – Security Objectives

Name	Description
O.IDAUTH	The TOE must uniquely identify and authenticate the claimed identity of all administrators, before granting an administrator access to TOE functions and data or, for certain specified services, to a connected network.
O.MEDIAT	The TOE must mediate the flow of all information between clients and servers located on internal and external networks governed by the TOE, disallowing passage of non-conformant protocols.
O.SECSTA	Upon initial start-up of the TOE or recovery from an interruption in TOE service, the TOE must not compromise its resources or those of any connected network.
O.SELPRO	The TOE must protect itself against attempts by unauthorized users to bypass, deactivate, or tamper with TOE security functions.
O.AUDREC	The TOE must provide a means to record a readable audit trail of security-related events, with accurate dates and times, and a means to search, sort, and order the audit trail based on relevant attributes.
O.ACCOUN	The TOE must provide user accountability for information flows through the TOE and for authorized administrator use of security functions related to audit.
O.SECFUN	The TOE must provide functionality that enables an authorized administrator to use the TOE security functions, and must ensure that only authorized administrators are able to access such functionality.

O.LIMEXT	The TOE must provide the means for an authorized administrator to control and limit access to TOE security functions by an authorized external IT entity.
O.VPN	The TOE must be able to protect the integrity and confidentiality of data transmitted to a peer authorized external IT entity via encryption and provide authentication for such data. Upon receipt of data from a peer authorized external IT entity, the TOE must be able to decrypt the data and verify that the received data accurately represents the data that was originally transmitted.

4.2 Security Objectives for the Environment

4.2.1 IT Security Objectives

The IT security objectives shown in Table 5 are to be satisfied by the environment.

Table 5 – IT Objectives

Name	Description
OE.TIME	The IT Environment will provide reliable timestamps to the TOE.
OE.VPN	The TOE Environment must be able to protect the integrity and confidentiality of data transmitted to a peer authorized external IT entity via encryption and provide authentication for such data. Upon receipt of data from a peer authorized external IT entity, the TOE Environment must be able to decrypt the data and verify that the received data accurately represents the data that was originally transmitted.

4.2.2 Non-IT Security Objectives

The non-IT environment security objectives shown in Table 6 are to be satisfied without imposing technical requirements on the TOE. That is, they will not require the implementation of functions in the TOE hardware and/or software. Thus, they will be satisfied largely through application of procedural or administrative measures.

Table 6 – Non-IT Security Objectives

Name	Description

NOE.NOEVIL	Authorized administrators are non-hostile and follow all administrator guidance.
NOE.GENPUR	The TOE only stores and executes security-relevant applications and only stores data required for its secure operation.
NOE.DIRECT	The TOE is available to authorized administrators only.
NOE.PHYSEC	The TOE is physically secure.
NOE.MODEXP	The threat of malicious attacks aimed at discovering exploitable vulnerabilities is considered low.
NOE.PUBLIC	The TOE does not host public data.
NOE.SINGEN	Information cannot flow among the internal and external networks unless it passes through the TOE.
NOE.REMACC	Authorized administrators may only access the TOE locally.
NOE.UPS	The TOE will be supported by an Uninterruptible Power Supply.
NOE.AUDSTG	Prior to audit storage exhaustion on the TOE, the audit records will be exported either via SMTP or to an external Syslog server for persistent storage.
NOE.FIPS	The TOE will only be installed and run on SonicWALL appliances that have been validated to FIPS 140-2 with the same version of the TOE.

5 Security Requirements

This section defines the SFRs and SARs met by the TOE as well as SFRs met by the TOE IT environment. These requirements are presented following the conventions identified in Section 1.3.1.

5.1 TOE Security Functional Requirements

This section specifies the SFRs for the TOE. This section organizes the SFRs by CC class. Table 7 identifies all SFRs implemented by the TOE and indicates the ST operations performed on each requirement.

Table 7 - TOE Security Functional Requirements

Name	Description	S	A	R	I
FAU_GEN.1	Audit data generation	✓	✓	✓	
FAU_SAR.1	Audit review		✓		
FAU_SAR.3	Selectable audit review	✓	✓		
FAU_STG.1	Protected audit trail storage	✓			
FCS_CKM.1	Cryptographic key generation		✓		
FCS_CKM.4	Cryptographic key destruction		✓		
FCS_COP.1	Cryptographic operation		✓		
FDP_IFC.1(a)	Subset information flow control		✓		✓
FDP_IFC.1(b)	Subset information flow control		✓		✓
FDP_IFF.1(a)	Simple security attributes		✓		✓
FDP_IFF.1(b)	Simple security attributes		✓		✓
FDP_ITC.1	Import of user data without security attributes		✓		
FIA_UAU.2	User authentication before any action			✓	
FIA_UID.2	User identification before any action			✓	
FMT_MOF.1	Management of security functions behaviour		✓	✓	

FMT_MSA.1	Management of security attributes	✓	✓		
FMT_MSA.2	Secure security attributes				
FMT_MSA.3(a)	Static attribute initialisation	✓	✓		✓
FMT_MSA.3(b)	Static attribute initialisation	✓	✓		✓
FMT_SMF.1	Specification of management functions		✓		
FMT_SMR.1	Security roles		✓		
FPT_RVM.1	Non-bypassability of the TSP				
FPT_SEP.1	TSF domain separation				
FTA_SSL.3	TSF-initiated termination		✓		

Note: S=Selection; A=Assignment; R=Refinement; I=Iteration

Section 5.1 contains the functional components from the CC Part 2 with the operations completed. For the conventions used in performing CC operations please refer to Section 1.3.1.

5.1.1 Class FAU: Security Audit

FAU_GEN.1 Audit Data Generation

Hierarchical to: No other components.

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) [*Blocked traffic, blocked websites, administrator account activity, VPN activity, firewall activity, firewall rule modifications, network access, IPS/GAV/SPY activity, and login attempts*].

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 **(when 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, [*no other information*].

Dependencies: FPT_STM.1 Reliable time stamps

FAU_SAR.1 Audit review

Hierarchical to: No other components.

FAU_SAR.1.1

The TSF shall provide [*authorised administrators*] with the capability to read [*all audit information*] from the audit records.

FAU_SAR.1.2

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

Dependencies: FAU_GEN.1 Audit data generation

FAU_SAR.3 Selectable audit review

Hierarchical to: No other components.

FAU_SAR.3.1

The TSF shall provide the ability to perform [*searches, sorting, ordering*] of audit data based on [*Priority, Category, Source IP or Interface, and Destination IP or interface*].

Dependencies: FAU_SAR.1 Audit review

FAU_STG.1 Protected audit trail storage

Hierarchical to: No other components.

FAU_STG.1.1

The TSF shall protect the stored audit records from unauthorised deletion.

FAU_STG.1.2

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

Dependencies: FAU_GEN.1 Audit data generation

5.1.2 Class FCS: Cryptographic Support

FCS_CKM.1 Cryptographic key generation

Hierarchical to: No other components.

FCS_CKM.1.1

The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [*cryptographic key generation algorithm – see table below*] and specified cryptographic key sizes [*cryptographic key sizes – see table below*] that meet the following: [*list of standards – see table below*].

Table 8: Cryptographic Key Generation Standards

Key Generation Type	Algorithm and Key Size	Standards (Certificate #)
PRNG	FIPS 186-2 Appendix 3.1 - RNG	FIPS 186-2 Appendix 3.1 (certificates #412, 413, 414, 415, 416)
Diffie-Hellman key agreement	Diffie-Hellman 1024 bit	RFC 2631

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

FCS_CKM.4 Cryptographic key destruction

Hierarchical to: No other components.

FCS_CKM.4.1

The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method [*zeroization*] that meets the following: [*FIPS 140-2 zeroization requirements*].

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

FCS_COP.1 Cryptographic operation

Hierarchical to: No other components.

FCS_COP.1.1

The TSF shall perform [*list of cryptographic operations – see table below*] in accordance with a specified cryptographic algorithm [*cryptographic algorithm – see table below*] and cryptographic key sizes [*cryptographic key sizes – see table below*] that meet the following: [*list of standards – see table below*].

Table 9: Cryptographic Operations

Cryptographic Operations	Cryptographic Algorithm	Key Sizes (bits)	Standards (Certificate #)
Digital signature verification	Digital Signature Algorithm (DSA)	1024	FIPS 186-2 (certificates #266, 267, 268, 269, 270)
	RSA	1024, 1536, 2048	FIPS 186-2 (certificates #327, 328, 329, 330, 331)
Symmetric encryption and decryption	Advanced Encryption Standard (AES) (CBC mode)	128, 192, 256	FIPS 197 (certificates #701, 702, 703, 704, 705)
	Triple-Data Encryption Standard (3DES) (TCBC mode)	3-key and 2-key	NIST SP 800-67, May 2004 (certificates #632, 633, 634, 635, 636)

Hashing	Secure Hash Algorithm1 (SHA -1)	Not Applicable	FIPS 180-2 (certificates #729, 730, 731, 732, 733)
Message Authentication	Keyed-Hash Message Authentication Code (HMAC) with Secure Hash 1 (SHA -1)	20 Bytes, truncated to 12 Bytes per RFC 2404	FIPS 198 (certificates #379, 380, 381, 382, 383)

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

5.1.3 Class FDP: User Data Protection

FDP_IFC.1(a) Subset information flow control

Hierarchical to: No other components.

FDP_IFC.1.1(a)

The TSF shall enforce the [*Traffic Information Flow Control SFP*[4]] on [

a) SUBJECTS: external IT entities that send or receive information through the TOE,

b) INFORMATION: traffic flowing through the TOE, and

c) OPERATIONS: ALLOW, DENY, DISCARD, PREVENT, DETECT].

Dependencies: FDP_IFF.1 Simple security attributes

FDP_IFC.1(b) Subset information flow control

Hierarchical to: No other components.

FDP_IFC.1.1(b)

The TSF shall enforce the [*Diffie-Hellman Information Flow Control SFP*] on [

a) SUBJECTS: external IT entities that send or receive information through the TOE,

b) INFORMATION: Diffie-Hellman public parameter for key exchange, and

c) OPERATIONS: ALLOW].

Dependencies: FDP_IFF.1 Simple security attributes

FDP_IFF.1(a) Simple security attributes

Hierarchical to: No other components.

FDP_IFF.1.1(a)

[4] Please note that the Traffic Information Flow Control SFP and the Diffie-Hellman Information Flow Control SFP are described in greater detail in the document, “SonicWALL SonicOS v5.0.1 on NSA Series and TZ Series Appliances Informal Security Policy Model”.

The TSF shall enforce the [*Traffic Information Flow Control SFP*] based on the following types of subject and information security attributes: [

SUBJECT (external IT entities) attributes:

1) *Internet Protocol (IP) address, and*

INFORMATION (traffic) attributes:

1) *source IP address,*
2) *destination IP address,*
3) *protocol type,*
4) *port number, and*
5) *port types or subtypes*].

FDP_IFF.1.2(a)

The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: [*ALLOW, DETECT rules contained in the administrator-defined Traffic Information Flow Control List*].

FDP_IFF.1.3(a)

The TSF shall enforce the [*additional SFP rules: a) restrict by time and b) prevent by security service*].

FDP_IFF.1.4(a)

The TSF shall provide the following [*no other capabilities*].

FDP_IFF.1.5(a)

The TSF shall explicitly authorise an information flow based on the following rules: [*no other rules*].

FDP_IFF.1.6(a)

The TSF shall explicitly deny an information flow based on the following rules: [*DENY, DISCARD, PREVENT rules contained in the administrator-defined Traffic Information Flow Control List*].

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

FDP_IFF.1(b) Simple security attributes

Hierarchical to: No other components.

FDP_IFF.1.1(b)

The TSF shall enforce the [*Diffie-Hellman Information Flow Control SFP*] based on the following types of subject and information security attributes: [

SUBJECT (external IT entities) attributes:

1) *Internet Protocol (IP) address, and*

INFORMATION (Diffie-Hellman public parameter for key exchange) attributes:

1) *none*].

FDP_IFF.1.2(b)

The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: [*none*].

FDP_IFF.1.3(b)

The TSF shall enforce the [*no other rules*].

FDP_IFF.1.4(b)

The TSF shall provide the following [*no other capabilities*].

FDP_IFF.1.5(b)

The TSF shall explicitly authorise an information flow based on the following rules: [*no other rules*].

FDP_IFF.1.6(b)

The TSF shall explicitly deny an information flow based on the following rules: [*no other rules*].

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

FDP_ITC.1 Import of user data without security attributes

Hierarchical to: No other components.

FDP_ITC.1.1

The TSF shall enforce the [*Diffie-Hellman Information Flow Control SFP*] when importing user data, controlled under the SFP, from outside of the TSC.

FDP_ITC.1.2

The TSF shall ignore any security attributes associated with the user data when imported from outside the TSC.

FDP_ITC.1.3

The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TSC: [*no additional importation control rules*].

Dependencies: [FDP_ACC.1 Subset access control, or
FDP_IFC.1 Subset information flow control]
FMT_MSA.3 Static attribute initialisation

5.1.4 Class FIA: Identification and Authentication

FIA_UAU.2 User authentication before any action

Hierarchical to: FIA_UAU.1

FIA_UAU.2.1

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

Dependencies: FIA_UID.1 Timing of identification

FIA_UID.2 User identification before any action

Hierarchical to: FIA_UID.1

FIA_UID.2.1

The TSF shall require each ~~user~~ **administrator** to identify itself before allowing any other TSF-mediated actions on behalf of that ~~user~~ **administrator**.

Dependencies: No dependencies

5.1.5 Class FMT: Security Management

FMT_MOF.1 Management of security functions behaviour

Hierarchical to: No other components.

FMT_MOF.1.1

The TSF shall restrict the ability to [*perform the action indicated in Table 10 below*] the functions [*in the Security Function column of Table 10 below*] to [*the roles as specified in Table 10 below*].

Table 10 - Management of Security Functions Behavior

Roles Security Function	Full Administrator Config Mode	Full Administrator Non-Config Mode	Full Administrator Read-Only Mode	Limited Administrator
Import Certificates	determine the behavior of, disable, enable, modify the behavior of	none	none	none
Generate Certificate Signing Requests	determine the behavior of, disable, enable, modify the behavior of	none	none	none
Export Certificates	determine the behavior of, disable, enable, modify the behavior of	none	none	none
Export Firmware Settings	determine the behavior of, disable, enable, modify the behavior of	enable	enable	none
Use Diagnostics	determine the behavior of, disable, enable, modify the behavior of	enable	enable	enable (except downloading TSR)

Download Tech Support Report (TSR)	determine the behavior of, disable, enable, modify the behavior of	enable	enable	none
Configure Network	determine the behavior of, disable, enable, modify the behavior of	none	none	enable
Flush ARP Cache	determine the behavior of, disable, enable, modify the behavior of	enable	none	enable
Set up DHCP Server	determine the behavior of, disable, enable, modify the behavior of	none	none	none
Renegotiate VPN Tunnels	determine the behavior of, disable, enable, modify the behavior of	enable	none	none
Log Accounts Off Appliance	determine the behavior of, disable, enable, modify the behavior of	enable	none	enable (for guest users only)
Unlock Locked-out Users	determine the behavior of, disable, enable, modify the behavior of	enable	none	none
Clear Log	determine the behavior of, disable, enable, modify the behavior of	enable	none	enable
Export Log	determine the behavior of, disable, enable, modify the behavior of	enable	enable	enable

Email Log	determine the behavior of, disable, enable, modify the behavior of	enable	none	enable
Filter Logs	determine the behavior of, disable, enable, modify the behavior of	enable	none	enable
Configure Log Categories	determine the behavior of, disable, enable, modify the behavior of	enable	none	enable
Configure Log Settings	determine the behavior of, disable, enable, modify the behavior of	none	none	enable
Generate Log Reports	determine the behavior of, disable, enable, modify the behavior of	enable	none	enable
Browse All Other User Interface Pages	determine the behavior of, disable, enable, modify the behavior of	enable	enable	none
Perform All Other TOE Configuration Activities	determine the behavior of, disable, enable, modify the behavior of	none	none	none

Dependencies: FMT_SMF.1 Specification of management functions
FMT_SMR.1 Security roles

FMT_MSA.1 Management of security attributes

Hierarchical to: No other components.

FMT_MSA.1.1

The TSF shall enforce the [*Traffic Information Flow Control SFP*] to restrict the ability to [*add or delete from the rules in the Traffic Information Flow Control list]*] the security attributes [*Source IP address, Destination IP address, Protocol Type, port number ,port type or subtype*] to [*Full Administrator Config Mode role*].

Dependencies: [FDP_ACC.1 Subset access control or
FDP_IFC.1 Subset information flow control]
FMT_SMF.1 Specification of management functions
FMT_SMR.1 Security roles

FMT_MSA.2 Secure security attributes

Hierarchical to: No other components.

FMT_MSA.2.1

The TSF shall ensure that only secure values are accepted for security attributes.

Dependencies: ADV_SPM.1 Informal TOE security policy model
[FDP_ACC.1 Subset access control or
FDP_IFC.1 Subset information flow control]
FMT_MSA.1 Management of security attributes
FMT_SMR.1 Security roles

FMT_MSA.3(a) Static attribute initialisation

Hierarchical to: No other components.

FMT_MSA.3.1(a)

The TSF shall enforce the [*Traffic Information Flow Control SFP*] to provide [*restrictive*] default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2(a)

The TSF shall allow the [*Full Administrator Config Mode role*] to specify alternative initial values to override the default values when an object or information is created.

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

FMT_MSA.3(b) Static attribute initialisation

Hierarchical to: No other components.

FMT_MSA.3.1(b)

The TSF shall enforce the [*Diffie-Hellman Information Flow Control SFP*] to provide [*permissive*] default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2(b)

The TSF shall allow the [*no role*] to specify alternative initial values to override the default values when an object or information is created.

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

FMT_SMF.1 Specification of Management Functions

Hierarchical to: No other components.

FMT_SMF.1.1

The TSF shall be capable of performing the following security management functions: [*Management of security functions and Management of security attributes*].

Dependencies: No Dependencies

FMT_SMR.1 Security roles

Hierarchical to: No other components.

FMT_SMR.1.1

The TSF shall maintain the roles [*Full Administrator Config Mode, Full Administrator Non-config Mode, Full Administrator Read-only Mode, Limited Administrator*].

FMT_SMR.1.2

The TSF shall be able to associate users with roles.

Dependencies: FIA_UID.1 Timing of identification

5.1.6 Class FPT: Protection of the TSF

FPT_RVM.1 Non-bypassability of the TSP

Hierarchical to: No other components.

FPT_RVM.1.1

The TSF shall ensure that TSP enforcement functions are invoked and succeed before each function within the TSC is allowed to proceed.

Dependencies: No dependencies

FPT_SEP.1 TSF domain separation

Hierarchical to: No other components.

FPT_SEP.1.1

The TSF shall maintain a security domain for its own execution that protects it from interference and tampering by untrusted subjects.

FPT_SEP.1.2

The TSF shall enforce separation between the security domains of subjects in the TSC.

Dependencies: No dependencies

5.1.7 Class FTA: TOE Access

FTA_SSL.3 TSF-initiated termination

Hierarchical to: No other components.

FTA_SSL.3.1

The TSF shall terminate an interactive session after a [*a configurable time interval of administrator inactivity at the Management Console ranging from 1 to 9999 minutes, defaulting to 5 minutes*].

Dependencies: No dependencies

5.2 Security Functional Requirements on the IT Environment

The TOE has the following security requirements for its IT environment. These requirements are presented following the conventions identified in Section 1.3.1.

Table 11 - TOE Environment Security Functional Requirements

Name	Description	S	A	R	I
FPT_STM.1	Reliable time stamps			✓	
FCS_FIPS.1 (EXP)	Cryptographic Dependency				

Note: S=Selection; A=Assignment; R=Refinement; I=Iteration

5.2.1 Class FCS: Cryptographic Dependency

FCS_FIPS.1 (EXP) FIPS

Hierarchical to: No other components.

FCS_FIPS.1.1 (EXP)

The TOE will only be installed and run on SonicWALL appliances that have been validated to FIPS 140-2 with the same version of the TOE.

Dependencies: No dependencies

5.2.2 Class FPT: Protection of the TOE Environment

FPT_STM.1 Reliable time stamps

Hierarchical to: No other components.

FPT_STM.1.1

The ~~TSF~~ **TOE Environment** shall be able to provide reliable time stamps for ~~its own~~ **the TOE's** use.

Dependencies: No dependencies

5.3 Assurance Requirements

This section defines the assurance requirements for the TOE. Assurance requirements are taken from the CC Part 3 and are EAL4 augmented with ALC_FLR.1. Table 12 – Assurance Requirements summarizes the requirements.

Table 12 – Assurance Requirements

Assurance Requirements	
Class ACM: Configuration management	ACM_AUT.1 Partial CM automation ACM_CAP.4 Generation support and acceptance procedures ACM_SCP.2 Problem tracking CM coverage
Class ADO: Delivery and operation	ADO_DEL.2 Detection of modification
	ADO_IGS.1 Installation, generation, and start-up procedures
Class ADV: Development	ADV_FSP.2 Fully defined external interfaces
	ADV_HLD.2 Security enforcing high-level design
	ADV_IMP.1 Subset of the implementation of the TSF
	ADV_LLD.1 Descriptive low-level design
	ADV_RCR.1 Informal correspondence demonstration
	ADV_SPM.1 Informal TOE security policy model
Class AGD: Guidance documents	AGD_ADM.1 Administrator guidance
	AGD_USR.1 User guidance
Class ALC : Life Cycle Support	ALC_DVS.1 Identification of security measures
	ALC_FLR.1 Basic Flaw Remediation
	ALC_LCD.1 Developer defined life-cycle model
	ALC_TAT.1 Well-defined development tools
Class ATE: Tests	ATE_COV.2 Analysis of coverage
	ATE_DPT.1 Testing: high-level design
	ATE_FUN.1 Functional testing
	ATE_IND.2 Independent testing – sample
Class AVA: Vulnerability assessment	AVA_MSU.2 Validation of analysis
	AVA_SOF.1 Strength of TOE security function evaluation
	AVA_VLA.2 Independent vulnerability analysis

6 TOE Summary Specification

This section presents information to detail how the TOE meets the functional and assurance requirements described in previous sections of this ST.

6.1 TOE Security Functions

Each of the security requirements and the associated descriptions correspond to the security functions. Hence, each function is described by how it specifically satisfies each of its related requirements. This serves to both describe the security functions and rationalize that the security functions satisfy the necessary requirements.

Table 13 – Mapping of TOE Security Functions to Security Functional Requirements

TOE Security Function	SFR ID	Description
Security Audit	FAU_GEN.1	Audit data generation
	FAU_SAR.1	Audit review
	FAU_SAR.3	Selectable audit review
	FAU_STG.1	Protected audit trail storage
Cryptographic Support	FCS_CKM.1	Cryptographic key generation
	FCS_CKM.4	Cryptographic key destruction
	FCS_COP.1	Cryptographic operation
	FCS_FIPS.1 (EXP)	Cryptographic Dependency
User Data Protection	FDP_IFC.1(a)	Subset information flow control

	FDP_IFC.1(b)	Subset information flow control
	FDP_IFF.1(a)	Simple security attributes
	FDP_IFF.1(b)	Simple security attributes
	FDP_ITC.1	Import of user data without security attributes
	FPT_STM.1	Reliable time stamps
Identification and Authentication	FIA_UAU.2	User authentication before any action
	FIA_UID.2	User identification before any action
Security Management	FMT_MOF.1	Management of security functions behaviour
	FMT_MSA.1	Management of security attributes
	FMT_MSA.2	Secure security attributes
	FMT_MSA.3(a)	Static attribute initialisation
	FMT_MSA.3(b)	Static attribute initialisation

	FMT_SMF.1	Specification of management functions
	FMT_SMR.1	Security roles
Protection of the TSF	FPT_RVM.1	Non-bypassability of the TSP
	FPT_SEP.1	TSF domain separation
TOE Access	FTA_SSL.3	TSF-initiated termination

6.1.1 Security Audit

The Security Audit function provides the TOE with the functionality for generation, storage, and viewing of audit records. As administrators manage and configure the TOE, their activities are tracked by recording audit records into the logs. All security-relevant configuration settings and changes are recorded to ensure accountability of the administrator's actions. All logs contain the date, time, event type, subject identity (when applicable) and outcome of the event for each record.

The TOE generates two types of audit logs: TOE management logs and user activity logs. TOE management logs contain information about administrator logins and changes to configuration parameters and access rules. User activity logs record blocked traffic, blocked websites, VPN activity, and firewall activity.

The TOE administrator has the ability to view all audit information from the audit logs, as well as search and sort the audit data. The logs can be searched based on priority, category, source IP address, and destination IP address. They can be sorted and ordered based on any of the fields listed in Table 14 below. The TOE protects the stored audit records from unauthorized deletion and modification.

The TOE audit records contain the following information:

Table 14 – Audit Record Contents

Field	Content
#	Log display identification number
Time	Time and date of the event
Priority	Level of priority associated with log event, such as Emergency or Error
Category	Type of traffic, such as Network Access or Authenticated Access
Message	Description of the event

Field	Content
Source	Source network and IP address
Destination	Destination network and IP address
Notes	Additional information about the event
Rule	Network Access Rule affected by event

TOE Security Functional Requirements Satisfied: [FAU_GEN.1, FAU_SAR.1, FAU_SAR.3, FAU_STG.1].

6.1.2 Cryptographic Support

The TOE provides IPSec VPN functionality for secure communications between two or more computers or protected networks over the public internet. This provides user authentication and encryption of information being passed through the VPN tunnel. The TOE uses the Internet Key Exchange (IKE) protocol for exchanging authentication information, and establishing the VPN tunnel. IKE uses either pre-shared secrets or digital certificates to authenticate peer devices. The TOE supports both version 1 and version 2 of IKE.

IKE version 1 uses a two phase process to secure the VPN tunnel. Phase 1 of IKE is the authentication phase. The nodes or gateways on either end of the tunnel authenticate with each other, exchange encryption and decryption keys, and establish the secure VPN tunnel. Phase 2 is the negotiation phase. Once authenticated, two nodes or gateways negotiate the methods of encryption and data verification (using a hash function) to be used on the data passed through the VPN. They then negotiate the number of SAs in the tunnel and the lifetimes allowed before requiring renegotiation of the encryption and decryption keys.

IKE version 2 also uses a two phase process to secure the tunnel. The initialization and authentication phase requires two message/response exchanges. The first pair of messages negotiates cryptographic algorithms, exchanges random values to guard against repeated messages, and performs a public key exchange. The second pair of messages authenticates the previous messages, exchanges identities and certificates, and establishes the first child SA. The negotiation phase of IKE version 2 consists of a single request/response pair, and may be initiated by either end of the SA after the initial exchanges are completed. All messages following the initial exchange are cryptographically protected using the cryptographic algorithms and keys negotiated in the first two messages of the IKE exchange.

The TOE shall only be installed and run on SonicWALL appliances that have been validated to FIPS 140-2 with the same version of the TOE.

Encryption methods implemented by the TOE include 3DES, AES-128, AES-192, and AES-256. The hashing methods used to authenticate the key include HMAC and SHA-1. Keys are generated and destroyed securely. All cryptographic operations are performed by a FIPS 140-2 validated cryptographic module.

TOE Security Functional Requirements Satisfied: [FCS_CKM.1, FCS_CKM.4, FCS_COP.1].

6.1.3 User Data Protection

The User Data Protection function implements functionality for TOE security functions and TOE security function policies related to protecting user data. The user data that the TOE is protecting is the information passing through the TOE. This functionality is provided by the application of firewall access rules. The Information Flow Control Security Functional Policy enforces rules on subjects that send traffic through the TOE, or receive traffic flowing through the TOE. The rules determine whether traffic should be passed from the sender to the receiver, denied passage, or discarded based on the following security attributes: source IP address, destination IP address, protocol type, port number, and port type or subtype.

When the TOE imports parameters for Diffie-Hellman key exchange, the TOE ignores[5] the security attributes associated with the user data when imported from outside the TSC.

Note: The explicit Security Functional Policies are fully described in the Informal Security Policy Model document (*SonicWALL SonicOS v5.0.1 on NSA Series and TZ Series Appliances: Informal Security Policy Model*).

TOE Security Functional Requirements Satisfied: [FDP_IFC.1, FDP_IFF.1].

6.1.4 Identification and Authentication

The Identification and Authentication function provides functionality to establish and verify a claimed administrator identity. This ensures that the administrator has the appropriate privileges associated with the assigned role. Only authenticated administrators will be allowed access to the TOE and TOE security functions. Administrators must be identified and authenticated prior to performing any other TSF-mediated actions on the TOE. For each administrator, the TOE stores the following security attributes in the database: username, password, and role. When TOE administrators enter a username and password at the Management Console, the information is passed to the TOE, where it is verified against the username and password stored in the TOE. If the provided username and password match, the TOE administrator is assigned the roles associated with that username.

TOE Security Functional Requirements Satisfied: [FIA_UAU.2, FIA_UID.2].

6.1.5 Security Management

The Security Management function specifies the management of several aspects of the TOE Security Function (TSF), including security function behavior and security attributes. The various management roles are also specified here: Full Administrator Config Mode, Full Administrator Non-config Mode, Full Administrator Read-only Mode, and Limited Administrator. Each role enforced by this TSF has different privileges to access and configure the behavior of the TOE. For example, Full Administrator Config Mode roles can perform any configuration of the TOE, whereas Limited Administrator roles can only configure log and network settings.

Adding or deleting security attributes (i.e., source or destination IP address or protocol type) from the rules in the Information Flow Control SFP is limited to administrators with the role Full Administrator Config Mode. Also, specifying alternative initial values for security attributes to override the default values is limited to administrators with the role Full Administrator Config Mode.

TOE Security Functional Requirements Satisfied: [FMT_MOF.1, FMT_MSA.1, FMT_MSA.3, FMT_SMF.1, FMT_SMR.1].

6.1.6 Protection of the TSF

The Protection of the TSF function provides the integrity and management of the mechanisms that provide the TSF. The security functional requirements in this evaluation are impossible to bypass because the TOE is designed in such a way that no access is possible without passing through key security features. These features include identification, authentication, and information flow control mediation. Non-bypassability of the TOE is provided by a combination of basic configuration and enforcement of security policy rules. It is not possible to perform any actions on the system without successfully authenticating. Once an administrator has been authenticated, that

[5] This statement refers to the SFR FDP_ITC.1.

administrator is bound to the appropriate privileges defined by the TOE. For any administrator to perform a TOE operation, an administrator in the Full Administrator Config Mode role must have granted that user the rights to perform that operation. These privileges are granted on a per administrator basis.

The TOE is an operating system that maintains a security domain for its own execution. Since all access control rights are checked by the TOE's mechanisms and the TOE uses unique attributes for each administrator, the TSF maintains separation between administrators. As an example, if an administrator in the Full Administrator Read-only Mode role attempts to edit a configuration, the command will be disallowed.

TOE Security Functional Requirements Satisfied: [FPT_RVM.1, FPT_SEP.1].

6.1.7 TOE Access

The TOE Access function specifies requirements for controlling the establishment of an administrator's session. The TSF provides this function by terminating an interactive management session after a configurable time interval of administrator inactivity at the Management Console. The default time interval is 5 minutes. This can be configured by an administrator to an interval between 1 and 9999 minutes. If an administrator's session is timed out, the administrator must log back in to the TOE to perform any further functions.

TOE Security Functional Requirements Satisfied: [FTA_SSL.3].

6.2 TOE Security Assurance Measures

EAL 4+ was chosen to provide a basic level of independently assured security. This section of the Security Target maps the assurance requirements of the TOE for a CC EAL 4+ level of assurance to the assurance measures used for the development and maintenance of the TOE. The following table provides a mapping of the appropriate documentation to the TOE assurance requirements.

Table 15 - Assurance Measures Mapping to TOE Security Assurance Requirements (SARs)

Assurance Component	Assurance Measure
ACM_AUT.1	SonicWALL SonicOS v5.0.1 on NSA Series and TZ Series Appliances - Configuration Management
ACM_CAP.4	SonicWALL SonicOS v5.0.1 on NSA Series and TZ Series Appliances - Configuration Management
ACM_SCP.2	SonicWALL SonicOS v5.0.1 on NSA Series and TZ Series Appliances - Configuration Management
ADO_DEL.2	SonicWALL SonicOS v5.0.1 on NSA Series and TZ Series Appliances - Secure Delivery

Assurance Component	Assurance Measure
ADO_IGS.1	SonicWALL Network Security Appliance E7500 Getting Started Guide SonicWALL Network Security Appliance E6500 Getting Started Guide SonicWALL Network Security Appliance E5500 Getting Started Guide SonicWALL Network Security Appliance 5000/4500/3500 SonicWALL TZ 190 Getting Started Guide SonicWALL TZ 190 Wireless Getting Started Guide SonicWALL TZ 180 Getting Started Guide SonicWALL TZ 180 Wireless Getting Started Guide
ADV_FSP.2	SonicWALL SonicOS v5.0.1 on NSA Series and TZ Series Appliances - TOE Architecture: Functional Specification, High Level Design, Low Level Design, and Representation Correspondence
ADV_HLD.2	SonicWALL SonicOS v5.0.1 on NSA Series and TZ Series Appliances - TOE Architecture: Functional Specification, High Level Design, Low Level Design, and Representation Correspondence
ADV_IMP.1	SonicWALL SonicOS v5.0.1 on NSA Series and TZ Series Appliances - TOE Architecture: Functional Specification, High Level Design, Low Level Design, and Representation Correspondence
ADV_LLD.1	SonicWALL SonicOS v5.0.1 on NSA Series and TZ Series Appliances - TOE Architecture: Functional Specification, High Level Design, Low Level Design, and Representation Correspondence
ADV_RCR.1	SonicWALL SonicOS v5.0.1 on NSA Series and TZ Series Appliances - TOE Architecture: Functional Specification, High Level Design, Low Level Design, and Representation Correspondence
ADV_SPM.1	SonicWALL SonicOS v5.0.1 on NSA Series and TZ Series Appliances - Informal Security Policy Model
AGD_ADM.1	SonicWALL SonicOS Enhanced 5.0 Administrator’s Guide
AGD_USR.1	(see AGD_ADM.1)
ALC_DVS.1	SonicWALL SonicOS v5.0.1 on NSA Series and TZ Series Appliances – Life Cycle
ALC_FLR.1	SonicWALL SonicOS v5.0.1 on NSA Series and TZ Series Appliances – Life Cycle
ALC_LCD.1	SonicWALL SonicOS v5.0.1 on NSA Series and TZ Series Appliances – Life Cycle
ALC_TAT.1	SonicWALL SonicOS v5.0.1 on NSA Series and TZ Series Appliances – Life Cycle

Assurance Component	Assurance Measure
ATE_COV.2	SonicWALL SonicOS v5.0.1 on NSA Series and TZ Series Appliances – Testing: Coverage, Depth
ATE_DPT.1	SonicWALL SonicOS v5.0.1 on NSA Series and TZ Series Appliances – Testing: Coverage, Depth
ATE_FUN.1	SonicWALL SonicOS v5.0.1 on NSA Series and TZ Series Appliances – Functional Tests SonicWALL SonicOS v5.0.1 on NSA Series and TZ Series Appliances – Functional Test Cases
AVA_MSU.2	SonicWALL SonicOS v5.0.1 on NSA Series and TZ Series Appliances - Vulnerability Assessment
AVA_SOF.1	SonicWALL SonicOS v5.0.1 on NSA Series and TZ Series Appliances - Vulnerability Assessment
AVA_VLA.2	SonicWALL SonicOS v5.0.1 on NSA Series and TZ Series Appliances - Vulnerability Assessment

6.2.1 ACM_CAP.4, ACM_AUT.1, and ACM_SCP.2: Configuration Management Document

The Configuration Management (CM) document provides a description of the various tools used to control the configuration items and how they are used internally at SonicWALL. This document provides a complete configuration item list and a unique referencing scheme for each configuration item. Additionally, the configuration management system is described including procedures that are used by developers to control and track changes that are made to the TOE. The documentation further details the TOE configuration items that are controlled by the configuration management system.

Partial Configuration Management automation (ACM_AUT.1) provides assurance that changes occur during development are authorized. The CM documentation describes how the CM system provides automated means to support the generation of the TOE and how automated tools are used in the CM system.

Problem tracking CM coverage (ACM_SCP.2) provides assurance that security flaws are not lost or forgotten. The CM documentation describes how security flaws are covered and tracked by SonicWALL's CM system.

6.2.2 ADO_DEL.2: Secure Delivery Document

The Delivery and Operation document provides a description of the secure delivery procedures implemented by SonicWALL to protect against TOE modification during product delivery. The Installation Documentation provided by SonicWALL details the procedures for installing the TOE and placing the TOE in a secure state offering the same protection properties as the master copy of the TOE. The Installation Documentation provides guidance to the TOE Users on configuring the TOE and how those TOE configurations affect the TSF.

6.2.3 ADO_IGS.1: Installation Guidance, AGD_ADM.1: Administrator Guidance, AGD_USR.1: User Guidance

The installation guidance document provides the procedures necessary for the secure installation, generation, and start-up of the TOE for administrators and users of the TOE.

The administrator guidance documentation provides detailed procedures for the administration of the TOE and description of the security functions provided by the TOE.

There is no User Guidance other than what might be contained in the administrator guidance, since the TOE operates transparently to the end users.

6.2.4 ADV_FSP.2: Fully defined external interfaces, ADV_HLD.2: Security enforcing high-level design, ADV_LLD.1: Low Level Design, ADV_IMP.1: Subset of the implementation of the TSF, and ADV_RCR.1: Informal correspondence demonstration.

The SonicWALL design documentation consists of several related design documents that address the components of the TOE at different levels of abstraction. The following design documents address the Development Assurance Requirements:

- The Functional Specification provides a description of the security functions provided by the TOE and a description of the external interfaces to the TSF. The Functional Specification covers the purpose and method of use and a list of effects, exceptions, and errors message for each external TSF interface.
- The High-Level Design provides a top level design specification that refines the TSF functional specification into the major constituent parts (subsystems) of the TSF. The high-level design identifies the basic structure of the TSF, the major elements, a listing of all interfaces, and the purpose and method of use for each interface.
- The Implementation Representation provides assurance that the TSF is unambiguously defined to a level of detail such that the TSF can be generated without further design decisions. It also describes the relationships between portions of the implementation.
- The Representation Correspondence demonstrates the correspondence between each of the TSF representations provided. This mapping is performed to show the functions traced from all of the adjacent pairs of TSF representation that are provided.

6.2.5 ADV_SPM.1: Informal TOE Security Policy Model

The Security Policy Model provides assurance that all of the security functions in the Functional Specification are sufficient to enforce the policies in the TSP. An informal model is provided for a subset of the TSP policies and the correspondence between the Functional Specification, the Security Policy Model, and the subset of policies is established.

6.2.6 ALC_DVS.1: Identification of security measures, ALC_FLR.1: Basic flaw remediation, ALC_LCD.1: Developer defined life-cycle model, and ALC_TAT.1: Well-defined development tools

Identification of security measures provides assurance that the TOE is developed in a secure environment. The Life Cycle Support documentation describes all the physical, procedural, personnel, and other security measures that are used to protect the TOE design and implementation in its development environment. It provides evidence that these security measures are followed during the development and maintenance of the TOE.

Providing basic flaw remediation provides assurance that the TOE will be maintained and supported, discovered security flaws will be tracked and corrected by the developer, and fixes will be issued to TOE users. The Flaw Remediation documentation describes the established procedures for accepting and acting upon all reports of security flaws and requests for corrections of those flaws. It also describes the internal process used to track, correct, and validate flaws.

The developer defined life-cycle model described the process used to develop the TOE. The life-cycle model is used throughout development and maintenance. The life-cycle documentation provides a description of the life-cycle model and an explanation on why the model is used is also documented.

The use of well-defined development tools prevents the use of incorrect or inconsistent development tools during TOE development. The development tools used by SonicWALL are described in the life cycle documentation. The selected implementation-dependent options of the development tools are described.

6.2.7 ATE_COV.2: Test Coverage Analysis, ATE_DPT.1: Test Depth Analysis, and ATE_FUN.1: Functional Testing

There are a number of components that make up the Test documentation. The Coverage Analysis demonstrates that testing is performed against the functional specification. The Coverage Analysis demonstrates the extent to which the TOE security functions were tested as well as the level of detail to which the TOE was tested. Test Plans and Test Procedures, which detail the overall efforts of the testing effort and break down the specific steps taken by a tester, are also provided in order to meet the assurance requirement Functional Testing.

Testing against the high-level design counters the risk of missing an error in the development of the TOE. This testing exercises specific internal interfaces. This ensures that the correct external behavior is a result of correctly operating internal mechanisms. The depth analysis demonstrates that the tests identified in the test documentation are sufficient to demonstrate that the TSF operates in accordance with its high-level design.

6.2.8 AVA_VLA.2: Vulnerability Analysis, AVA_MSU.2: Misuse Guidance, and AVA_SOF.1: Strength of Function Analysis

A Vulnerability Analysis is provided to demonstrate ways in which an entity could violate the TSP and provide a list of identified vulnerabilities. Additionally, this document provides evidence of how the TOE is resistant to obvious attacks.

The Misuse Guidance documentation examines the guidance documentation and provides assurance no misleading, unreasonable, or conflicting instructions are present. It identifies all possible modes of operation of the TOE, their consequences, and implications for maintaining secure operation. The Vulnerability Analysis documentation describes the analysis of the TOE deliverables performed to search for ways in which a user can violate the TSP, and the disposition of the identified vulnerabilities.

The Strength of TOE Security Function Analysis demonstrates the strength of the probabilistic or permutational mechanisms employed to provide security functions within the TOE and how they exceed the minimum Strength of Function (SOF) requirements.

7 Protection Profile Claims

This section provides the identification and justification for any Protection Profile conformance claims.

7.1 Protection Profile Reference

There are no protection profile claims for this ST.

8 Rationale

This section provides the rationale for the selection of the security requirements, objectives, assumptions, and threats. In particular, it shows that the security requirements are suitable to meet the security objectives, which in turn are shown to be suitable to cover all aspects of the TOE security environment.

8.1 Security Objectives Rationale

This section provides a rationale for the existence of each assumption and threat statement that compose the ST. The tables in Sections 8.1.1 and 8.1.2 demonstrate the mappings between the assumptions and threats to the security objectives are complete. The following discussion provides detailed evidence of coverage for each assumption and threat.

8.1.1 Security Objectives Rationale Relating to Threats

Table 16 - Security Objectives Rationale Relating to Threats

Threats	Objectives	Rationale
T.ASPOOF An unauthorized entity may carry out spoofing in which information flows through the TOE into a connected network by using a spoofed source address.	O.MEDIAT The TOE must mediate the flow of all information between clients and servers located on internal and external networks governed by the TOE, disallowing passage of non-conformant protocols.	The O.MEDIAT objective addresses the T.ASPOOF threat by mediating the flow of all information between clients and servers located on internal and external networks governed by the TOE, disallowing passage of non-conformant protocols.
T.AUDACC Persons may not be accountable for the actions that they conduct, thus allowing an attacker to escape detection.	O.AUDREC The TOE must provide a means to record a readable audit trail of security-related events, with accurate dates and times, and a means to search, sort, and order the audit trail based on relevant attributes.	The O.AUDREC objective addresses the T.AUDACC threat by requiring the TOE to provide a readable audit trail of security-related events, thereby allowing authorized administrators to discover attacker actions.
	O.ACCOUN The TOE must provide user accountability for information flows through the TOE and for authorized administrator use of security functions related to audit.	The O.ACCOUN objective addresses the T.AUDACC threat by requiring the TOE to provide user accountability for information flows through the TOE and for authorized administrator use of security functions related to audit.
	OE.TIME The IT Environment will provide reliable timestamps to the TOE.	The OE.TIME environmental objective addresses the T.AUDACC threat by requiring the TOE Environment to provide reliable timestamps to the TOE, for use in audit records. Authorized administrators may use the audit records to identify attacker actions.

T.SELPRO An unauthorized user may read, modify, or destroy security critical TOE configuration data stored on the TOE.	O.SECSTA Upon initial start-up of the TOE or recovery from an interruption in TOE service, the TOE must not compromise its resources or those of any connected network.	The O.SECSTA objective addresses the T.SELPRO threat by requiring that the TOE not compromise its resources or those of any connected network upon initial start-up or recovery from interruption in TOE service.
	O.SELPRO The TOE must protect itself against attempts by unauthorized users to bypass, deactivate, or tamper with TOE security functions.	The O.SELPRO objective addresses the T.SELPRO threat by requiring that the TOE protect itself from attempts by unauthorized users to bypass, deactivate, or tamper with TOE security functions.
T.REPEAT An unauthorized person may repeatedly try to guess authentication data used for performing I&A functionality in order to use this information to launch attacks on the TOE.	O.SECFUN The TOE must provide functionality that enables an authorized administrator to use the TOE security functions, and must ensure that only authorized administrators are able to access such functionality.	The O.SECFUN objective addresses the T.REPEAT threat by requiring the TOE to ensure that only authorized administrators are able to access the TOE security functions.
T.NOAUTH An unauthorized user may attempt to bypass the security of the TOE so as to access and use security functions and/or non-security functions provided by the TOE.	O.IDAUTH The TOE must uniquely identify and authenticate the claimed identity of all administrators, before granting an administrator access to TOE functions and data or, for certain specified services, to a connected network.	The O.IDAUTH objective addresses the T.NOAUTH threat by requiring that the TOE uniquely identify and authenticate the claimed identity of all administrators before granting access to TOE functions and data, or to a connected network.
	O.SECSTA Upon initial start-up of the TOE or recovery from an interruption in TOE service, the TOE must not compromise its resources or those of any connected network.	The O.SECSTA objective addresses the T.NOAUTH threat by requiring the TOE to protect its resources and those of any connected network from compromise upon initial start-up of the TOE or recovery from an interruption in TOE service.
	O.SELPRO The TOE must protect itself against attempts by unauthorized users to bypass, deactivate, or tamper with TOE security functions.	The O.SELPRO objective addresses the T.NOAUTH threat by requiring the TOE to protect itself from attempts by unauthorized users to bypass, deactivate, or tamper with TOE security functions.
	O.SECFUN The TOE must provide functionality that enables an authorized administrator to use the TOE security functions, and must ensure that only authorized administrators are able to	The O.SECFUN objective addresses the T.NOAUTH threat by requiring the TOE to provide functionality that enables an authorized administrator to use the TOE security functions, and ensure that only authorized administrators are able to access such

	access such functionality.	functionality.
	O.LIMEXT The TOE must provide the means for an authorized administrator to control and limit access to TOE security functions by an authorized external IT entity.	The O.LIMEXT objective addresses the T.NOAUTH threat by requiring the TOE to provide a means for an authorized administrator to control and limit access to TOE security functions by an authorized external IT entity.
	O.VPN The TOE must be able to protect the integrity and confidentiality of data transmitted to a peer authorized external IT entity via encryption and provide authentication for such data. Upon receipt of data from a peer authorized external IT entity, the TOE must be able to decrypt the data and verify that the received data accurately represents the data that was originally transmitted.	The O.VPN objective addresses the T.NOAUTH threat by requiring that the TOE protect the integrity and confidentiality of data through the TOE via encryption.
	OE.VPN The TOE Environment must be able to protect the integrity and confidentiality of data transmitted to a peer authorized external IT entity via encryption and provide authentication for such data. Upon receipt of data from a peer authorized external IT entity, the TOE Environment must be able to decrypt the data and verify that the received data accurately represents the data that was originally transmitted.	The OE.VPN objective addresses the T.NOAUTH threat by requiring that the TOE Environment protect the integrity and confidentiality of data through the TOE via encryption.
T.MEDIAT An unauthorized person may send impermissible information through the TOE which results in the exploitation of resources on the internal network.	O.MEDIAT The TOE must mediate the flow of all information between clients and servers located on internal and external networks governed by the TOE, disallowing passage of non-conformant protocols.	The O.MEDIAT objective addresses the T.MEDIAT threat by ensuring that the TOE mediate the flow of all information between clients and servers located on internal and external networks governed by the TOE.
T.AUDFUL An unauthorized user may cause audit records to be lost or prevent future records from being recorded by taking actions to exhaust audit storage capacity, thus masking an	O.SELPRO The TOE must protect itself against attempts by unauthorized users to bypass, deactivate, or tamper with TOE security functions.	The O.SELPRO objective addresses the T.AUDFUL threat by requiring that the TOE protect itself from attempts by unauthorized users to bypass, deactivate, or tamper with TOE security functions.

attacker's actions.	O.SECFUN The TOE must provide functionality that enables an authorized administrator to use the TOE security functions, and must ensure that only authorized administrators are able to access such functionality.	The O.SECFUN objective addresses the T.AUDFUL threat by requiring that only authorized administrators are able to access TOE security functions, including modification or deletion of the audit records.
T.NACCESS An unauthorized person or external IT entity may be able to view data that is transmitted between the TOE and a remote authorized external IT entity.	O.VPN The TOE must be able to protect the integrity and confidentiality of data transmitted to a peer authorized external IT entity via encryption and provide authentication for such data. Upon receipt of data from a peer authorized external IT entity, the TOE must be able to decrypt the data and verify that the received data accurately represents the data that was originally transmitted.	The O.VPN objective addresses the T.NACCESS threat by ensuring that the TOE protects the integrity and confidentiality of data transmitted to a peer authorized external IT entity via encryption and provides authentication for such data.
	OE.VPN The TOE Environment must be able to protect the integrity and confidentiality of data transmitted to a peer authorized external IT entity via encryption and provide authentication for such data. Upon receipt of data from a peer authorized external IT entity, the TOE Environment must be able to decrypt the data and verify that the received data accurately represents the data that was originally transmitted.	The OE.VPN objective addresses the T.NACCESS threat by ensuring that the TOE Environment protects the integrity and confidentiality of data transmitted to a peer authorized external IT entity via encryption and provides authentication for such data.
T.NMODIFY An unauthorized person or external IT entity may modify data that is transmitted between the TOE and a remote authorized external entity.	O.VPN The TOE must be able to protect the integrity and confidentiality of data transmitted to a peer authorized external IT entity via encryption and provide authentication for such data. Upon receipt of data from a peer authorized external IT entity, the TOE must be able to decrypt the data and verify that the received data accurately represents the data that was originally transmitted.	The O.VPN objective addresses the T.NMODIFY threat by ensuring that the TOE protects the integrity and confidentiality of data transmitted to a peer authorized external IT entity via encryption and provides authentication for such data.
	OE.VPN The TOE Environment must be able to protect the integrity and confidentiality of data transmitted to a peer	The OE.VPN objective addresses the T.NMODIFY threat by ensuring that the TOE Environment protects the integrity and confidentiality of data transmitted to a peer authorized

	authorized external IT entity via encryption and provide authentication for such data. Upon receipt of data from a peer authorized external IT entity, the TOE Environment must be able to decrypt the data and verify that the received data accurately represents the data that was originally transmitted.	external IT entity via encryption and provides authentication for such data.

8.1.2 Security Objectives Rationale Relating to Assumptions

Table 17 - Security Objectives Rationale Relating to Assumptions

Assumptions	Objectives	Rationale
A.NOEVIL Authorized administrators are non-hostile and follow all administrator guidance.	NOE.NOEVIL Authorized administrators are non-hostile and follow all administrator guidance.	The NOE.NOEVIL objective ensures that authorized administrators are non-hostile and follow all administrator guidance.
A.GENPUR The TOE only stores and executes security-relevant applications and only stores data required for its secure operation.	NOE.GENPUR The TOE only stores and executes security-relevant applications and only stores data required for its secure operation.	The NOE.GENPUR objective ensures that the TOE only stores and executes security-relevant applications and only stores data required for its secure operation.
A.DIRECT The TOE is available to authorized administrators only.	NOE.DIRECT The TOE is available to authorized administrators only.	The NOE.DIRECT objective ensures that the TOE is available to authorized administrators only.
A.PHYSEC The TOE is physically secure.	NOE.PHYSEC The TOE is physically secure.	The NOE.PHYSEC objective ensures that the TOE is physically secure.
A.MODEXP The threat of malicious attacks aimed at discovering exploitable vulnerabilities is considered low.	NOE.MODEXP The threat of malicious attacks aimed at discovering exploitable vulnerabilities is considered low.	The NOE.MODEXP objective ensures that the threat of malicious attacks aimed at discovering exploitable vulnerabilities is low.
A.PUBLIC The TOE does not host public data.	NOE.PUBLIC The TOE does not host public data.	The NOE.PUBLIC objective ensures that the TOE does not host public data.
A.SINGEN	NOE.SINGEN	The NOE.SINGEN objective ensures that information cannot flow among

Information cannot flow among the internal and external networks unless it passes through the TOE.	Information cannot flow among the internal and external networks unless it passes through the TOE.	the internal and external networks unless it passes through the TOE.
A.REMACC Authorized administrators may only access the TOE locally.	NOE.REMACC Authorized administrators may only access the TOE locally.	The NOE.REMACC objective ensures that authorized administrators may only access the TOE locally.
A.UPS The TOE will be supported by an Uninterruptible Power Supply.	NOE.UPS The TOE will be supported by an Uninterruptible Power Supply.	The NOE.UPS objective ensures that the TOE will not experience power failure, thereby ensuring that the audit records will be retained in RAM until the TOE exports it via SMTP or to a Syslog Server.
A.AUDSTG Prior to audit storage exhaustion on the TOE, the audit records will be exported either via SMTP or to an external Syslog server for persistent storage.	NOE.AUDSTG Prior to audit storage exhaustion on the TOE, the audit records will be exported either via SMTP or to an external Syslog server for persistent storage.	The NOE.AUDSTG objective ensures that the audit records will be exported via SMTP or to an external Syslog server prior to the filling of the audit file on the TOE.
A.FIPS The TOE will only be installed and run on SonicWALL appliances that have been validated to FIPS 140-2 with the same version of the TOE.	NOE.FIPS The TOE will only be installed and run on SonicWALL appliances that have been validated to FIPS 140-2 with the same version of the TOE.	The NOE.FIPS objective ensures that the TOE will only be installed on SonicWALL appliances that have been validated to FIPS 140-2 on the same version of the TOE.

8.1.3 Security Objectives Rationale Relating to Policies

There are no Organizational Policies.

8.2 Security Functional Requirements Rationale

The following discussion provides detailed evidence of coverage for each security objective.

8.2.1 Rationale for Security Functional Requirements of the TOE Objectives

Table 18 - Rationale for Security Functional Requirements of the TOE Objectives

Objective	Requirements Addressing the Objective	Rationale
O.IDAUTH	FIA_UAU.2	FIA_UAU.2 meets this objective by requiring that all administrators be

The TOE must uniquely identify and authenticate the claimed identity of all administrators, before granting an administrator access to TOE functions and data or, for certain specified services, to a connected network.	User authentication before any action	successfully authenticated before allowing any other TSF-mediated actions on behalf of that administrator.
	FIA_UID.2 User identification before any action	FIA_UID.2 meets this objective by requiring that all administrators be successfully identified before allowing any other TSF-mediated actions on behalf of that administrator.
	FTA_SSL.3 TSF-initiated termination	FTA_SSL.3 meets this objective by terminating an interactive session after a configurable time interval of administrator inactivity at the Management Console. The administrator must then login again to access the TOE.
O.MEDIAT The TOE must mediate the flow of all information between clients and servers located on internal and external networks governed by the TOE, disallowing passage of non-conformant protocols.	FCS_COP.1 Cryptographic operation	FCS_COP.1 meets this objective by ensuring that all traffic requiring cryptographic operations has access to the cryptographic module.
	FDP_IFC.1(a) Subset information flow control	FDP_IFC.1 meets this objective by specifying the rules by which subjects will allow or disallow information to flow to and from other subjects.
	FDP_IFC.1(b) Subset information flow control	FDP_IFC.1 meets this objective by specifying the rules by which subjects will allow or disallow information to flow to and from other subjects.
	FDP_IFF.1(a) Simple security attributes	FDP_IFF.1 meets this objective by specifying the rules by which subjects will allow or disallow information to flow to and from other subjects.
	FDP_IFF.1(b) Simple security attributes	FDP_IFF.1 meets this objective by specifying the rules by which subjects will allow or disallow information to flow to and from other subjects.
	FMT_MSA.1 Management of security attributes	FMT_MSA.1 meets this objective by enforcing the Information Flow Control Security Functional Policy, which restricts the ability to add or delete security attributes in the Information Flow Control List to the Full Administrator in Config Mode role.
O.SECSTA	FAU_STG.1	FAU_STG.1 meets this objective by ensuring that the audit records are

Upon initial start-up of the TOE or recovery from an interruption in TOE service, the TOE must not compromise its resources or those of any connected network.	Protected audit trail storage	protected from unauthorized modification and deletion.
	FMT_MOF.1 Management of security functions behaviour	FMT_MOF.1 meets this objective by requiring that TOE functions may only be accessed by authorized roles.
	FMT_MSA.1 Management of security attributes	FMT_MSA.1 meets this objective by enforcing the Information Flow Control Security Functional Policy, which restricts the ability to add or delete security attributes in the Information Flow Control List to the Full Administrator in Config Mode role.
	FMT_MSA.3(a) Static attribute initialisation	FMT_MSA.3 meets this objective by enforcing the Traffic Information Flow Control Security Functional Policy to provide restrictive default values for security attributes.
	FPT_RVM.1 Non-bypassability of the TSP	FPT_RVM.1 meets this objective by ensuring that TOE Security Policy enforcement functions are invoked and succeed before each function within the TOE Scope of Control is allowed to proceed.
O.SELPRO The TOE must protect itself against attempts by unauthorized users to bypass, deactivate, or tamper with TOE security functions.	FAU_STG.1 Protected audit trail storage	FAU_STG.1 meets this objective by ensuring the audit records are protected from unauthorized modification or deletion.
	FPT_RVM.1 Non-bypassability of the TSP	FPT_RVM.1 meets this objective by ensuring that TOE Security Policy enforcement functions are invoked and succeed before each function within the TOE Scope of Control is allowed to proceed.
	FPT_SEP.1 TSF domain separation	FPT_SEP.1 meets this objective by requiring that the TOE maintain a security domain for the TSF's execution that protects it from interference and tampering by untrusted subjects.
O.AUDREC The TOE must provide a means to record a readable audit trail of security-related events, with accurate dates and times, and a	FAU_GEN.1 Audit data generation	FAU_GEN.1 meets this objective by providing an audit trail listing all security-relevant actions on the TOE and on the information passing through the TOE.

means to search, sort, and order the audit trail based on relevant attributes.	FAU_SAR.1 Audit review	FAU_SAR.1 meets this objective by ensuring that authorized administrators are able to read and interpret all audit information from the audit records.
	FAU_SAR.3 Selectable audit review	FAU_SAR.3 meets this objective by ensuring the administrators can search, sort, and order the audit data based on Priority, Category, Source IP, and Destination IP.
O.ACCOUN The TOE must provide user accountability for information flows through the TOE and for authorized administrator use of security functions related to audit.	FAU_GEN.1 Audit data generation	FAU_GEN.1 meets this objective by providing an audit trail listing all security-relevant user and administrator actions on the TOE and on the information passing through the TOE.
	FIA_UID.2 User identification before any action	FIA-UID.2 meets this objective by requiring that all administrators be successfully identified before allowing any other TSF-mediated actions on behalf of that administrator.
O.SECFUN The TOE must provide functionality that enables an authorized administrator to use the TOE security functions, and must ensure that only authorized administrators are able to access such functionality.	FAU_GEN.1 Audit data generation	FAU_GEN.1 meets this objective by providing an audit trail listing all access to TOE security functions.
	FAU_STG.1 Protected audit trail storage	This objective is met by FAU_STG.1 because it ensures that the audit records are protected from unauthorized modification and deletion, thereby enabling authorized administrators to verify that only authorized administrators are accessing the TOE security functions.
	FIA_UAU.2 User authentication before any action	FIA_UAU.2 meets this objective by requiring that all administrators be successfully authenticated before allowing any other TSF-mediated actions on behalf of that administrator.
	FMT_MOF.1 Management of security functions behaviour	FMT_MOF.1 meets this objective by restricting access and performance of TOE security functions to authorized identified roles.
	FMT_MSA.1 Management of security attributes	FMT_MSA.1 meets this objective by enforcing the Information Flow Control Security Functional Policy, which restricts the ability to add or delete

		security attributes in the Information Flow Control List to the Full Administrator in Config Mode role.
	FMT_MSA.3(a) Static attribute initialisation	FMT_MSA.3 meets this objective by enforcing the Trafffic Information Flow Control Security Functional Policy to provide restrictive default values for security attributes.
	FMT_SMF.1 Specification of management functions	FMT_SMF.1 meets this objective by requiring that the TOE provide Management of Security Functions and Management of Security Attributes.
	FMT_SMR.1 Security roles	FMT_SMR.1 meets this objective by requiring that the TOE maintain security roles.
O.LIMEXT The TOE must provide the means for an authorized administrator to control and limit access to TOE security functions by an authorized external IT entity.	FMT_MOF.1 Management of security functions behaviour	FMT_MOF.1 meets this objective by restricting the ability to access and perform security functions to authorized identified roles.
	FMT_SMF.1 Specification of management functions	FMT_SMF.1 meets this objective by requiring that the TOE provide Management of Security Functions and Management of Security Attributes.
O.VPN The TOE must be able to protect the integrity and confidentiality of data transmitted to a peer authorized external IT entity via encryption and provide authentication for such data. Upon receipt of data from a peer authorized external IT entity, the TOE must be able to decrypt the data and verify that the received data accurately represents the data that was originally transmitted.	FCS_CKM.1 Cryptographic key generation	FCS_CKM.1 meets this objective by ensuring that cryptographic keys are generated in accordance with approved cryptographic key generation algorithms and key sizes.
	FCS_CKM.4 Cryptographic key destruction	FCS_CKM.4 meets this objective by ensuring that the cryptographic keys used by the TOE are destroyed in accordance with specified cryptographic key destruction methods.
	FCS_COP.1 Cryptographic operation	FCS_COP.1 meets this objective by performing cryptographic operations in accordance with specified cryptographic algorithms and key sizes.
	FDP_ITC.1 Import of user data without security	FDP_ITC.1 meets this objective by protecting the confidentiality of the Diffie-Hellman key exchange public

	attributes	parameter.
	FMT_MSA.2 Secure security attributes	FMT_MSA.2 meets this objective by requiring that only encrypted data with valid keys are decrypted.
	FMT_MSA.3(b) Static attribute initialisation	FMT_MSA.3(b) meets this objective by protecting the Diffie-Hellman public parameter during key exchange.

8.2.2 Rationale for Security Functional Requirements of the IT Environment

Table 19 - Rationale for Security Functional Requirements of the IT Environment

Objective	Requirements Addressing the Objective	Rationale
OE.TIME The IT Environment will provide reliable timestamps to the TOE.	FPT_STM.1 Reliable time stamps	FPT_STM.1 meets this objective by requiring that the TOE Environment provide timestamps to the TOE.
OE.VPN The TOE Environment must be able to protect the integrity and confidentiality of data transmitted to a peer authorized external IT entity via encryption and provide authentication for such data. Upon receipt of data from a peer authorized external IT entity, the TOE Environment must be able to decrypt the data and verify that the received data accurately represents the data that was originally transmitted.	FCS_FIPS.1 (EXP) Cryptographic Dependency	FCS_FIPS.1 meets this objective by requiring that the TOE will only be installed and run on SonicWALL appliances that have been validated to FIPS 140-2 with the same version of the TOE.

8.3 Security Assurance Requirements Rationale

EAL4+ was selected because it is best suited to addressing the stated security objectives. EAL4+ challenges vendors to use best (rather than average) commercial practices. Eal4+ allows the vendor to evaluate their product at a detailed level while avoiding the non-trivial expense and rigor of higher assurance levels, while still benefitting from the Common Criteria Recognition Agreement. The chosen assurance level is appropriate for the threats defined in the environment.

The augmentation of ALC_FLR.1 was chosen to give greater assurance of the developer’s on-going flaw remediation processes.

8.4 Rationale for Explicitly-defined Security Functional Requirements

FCS_FIPS was created to compensate for the boundary differences between the FIPS boundary and the CC boundary of the TOE. The FIPS boundary includes hardware components, such as a hardware accelerator, whereas the CC boundary is firmware-only.

8.5 Rationale for Refinements of Security Functional Requirements

The following refinements of Security Functional Requirements from CC version 2.3 have been made to clarify the content of the SFRs, and make them easier to read:

The term “when applicable” has been added to the FAU_GEN.1.2 (Section 5.1.1) component to clarify that subject identity is only recorded in an audit record when there is a subject identity associated with the record.

The term “user” has been refined to “administrator” in the FIA_UAU.2 and FIA_UID.2 SFRs in section 5.1.4.

The title “Class FPT: Protection of the TSF” has been refined to “Class FPT: Protection of the TOE Environment” in Section 5.2.2.

The term “TSF” has been refined to “TOE Environment” in Section 5.2.2.

8.6 Dependency Rationale

This ST does satisfy all the requirement dependencies of the Common Criteria. Table 20 lists each requirement to which the TOE claims conformance with a dependency and indicates whether the dependent requirement was included. As the table indicates, all dependencies have been met.

Table 20 - Functional Requirements Dependencies

SFR ID	Dependencies	Dependency Met	Rationale
FAU_GEN.1	FPT_STM.1	✓	
FAU_SAR.1	FAU_GEN.1	✓	
FAU_SAR.3	FAU_SAR.1	✓	
FAU_STG.1	FAU_GEN.1	✓	
FCS_CKM.1	FCS_COP.1	✓	
	FCS_CKM.4	✓	
	FMT_MSA.2	✓	
FCS_CKM.4	FCS_CKM.1	✓	

	FMT_MSA.2	✓	
FCS_COP.1	FCS_CKM.1	✓	
	FMT_MSA.2	✓	
	FCS_CKM.4	✓	
FDP_IFC.1(a)	FDP_IFF.1(a)	✓	
FDP_IFC.1(b)	FDP_IFF.1(b)	✓	
FDP_IFF.1(a)	FMT_MSA.3(a)	✓	
	FDP_IFC.1(a)	✓	
FDP_IFF.1(b)	FDP_IFC.1(b)	✓	
	FMT_MSA.3(b)	✓	
FDP_ITC.1	FMT_MSA.3(b)	✓	
	FDP_IFC.1(b)	✓	
FIA_UAU.2	FIA_UID.1	✓	Although FIA_UID.1 is not included, FIA_UID.2, which is hierarchical to FIA_UID.1 is included. This satisfies this dependency.
FIA_UID.2	No dependencies		
FMT_MOF.1	FMT_SMR.1	✓	
	FMT_SMF.1	✓	
FMT_MSA.1	FMT_SMR.1	✓	
	FMT_SMF.1	✓	
	FDP_IFC.1	✓	
FMT_MSA.2	FMT_SMR.1	✓	

	FDP_IFC.1(a)	✓	
	ADV_SPM.1	✓	
	FMT_MSA.1	✓	
FMT_MSA.3(a)	FMT_MSA.1	✓	
	FMT_SMR.1	✓	
FMT_MSA.3(b)	FMT_SMR.1	✓	
	FMT_MSA.1	✓	
FMT_SMF.1	No dependencies		
FMT_SMR.1	FIA_UID.1	✓	Although FIA_UID.1 is not included, FIA_UID.2, which is hierarchical to FIA_UID.1 is included. This satisfies this dependency.
FPT_RVM.1	No dependencies		
FPT_SEP.1	No dependencies		
FTA_SSL.3	No dependencies		
FPT_STM.1	No dependencies		
FCS_FIPS.1 (EXP)	No dependencies		

8.7 TOE Summary Specification Rationale

8.7.1 TOE Summary Specification Rationale for the Security Functional Requirements

Each subsection in the TOE Security Functions (Section 6.1) describes a security function of the TOE. Each description is organized by sets of requirements with rationale that indicates how these requirements are satisfied by aspects of the corresponding security function. The set of security functions work together to satisfy all of the security functional requirements and assurance requirements. Furthermore, all of the security functions are necessary in order for the TSF to provide the required security functionality. This section, in conjunction with the TOE Summary Specification section, provides evidence that the security functions are suitable to fulfill the TOE security requirements.

Table 21 identifies the relationship between security requirements and security functions, showing that all security requirements are addressed and all security functions are necessary (i.e., they correspond to at least one security requirement).

The only security mechanism that is realized by a probabilistic or permutational implementation is the password mechanism. For an analysis of the SOF, refer to Strength of Function Rationale, Section 8.8.

Table 21 - Mapping of Security Functional Requirements to TOE Security Functions

TOE Security Function	SFR	Rationale
Security Audit	FAU_GEN.1	This requires that appropriate audit records are generated. The TOE generates audit messages automatically (without outside intervention) when an auditable event occurs.
	FAU_SAR.1	This requires that the audit records be viewable by authorized users. The TOE allows authorized administrators to view the audit records through a graphical interface.
	FAU_SAR.3	This requires that the TOE provide the capability for the administrator to search, sort, and order the audit data. The TOE allows authorized administrators to search, sort, and order the audit data through a graphical interface.
	FAU_STG.1	This requires that the audit records be protected from unauthorized modification and deletion. The TOE stores audit records on a remote syslog server. Logs cannot be modified from the TOE when they are stored on the syslog server.
Cryptographic Support	FCS_CKM.1	This requires that the TOE generate cryptographic keys in accordance with the FIPS 140-2 standard. The TOE includes a FIPS 140-2 cryptographic module that handles all cryptographic functionality.
	FCS_CKM.4	This requires that the TOE destroy cryptographic keys in accordance with the FIPS 140-2 standard. The TOE

		includes a FIPS 140-2 cryptographic module that handles all cryptographic functionality.
	FCS_COP.1	This requires that the TOE perform cryptographic operations using cryptographic algorithms meeting FIPS algorithm standards. The TOE includes a FIPS 140-2 cryptographic module that handles all cryptographic functionality.
User Data Protection	FDP_IFC.1(a)	This requires that the TOE enforce a Traffic Information Flow Control Security Functional Policy. The TOE applies administrator-defined firewall rules to the traffic flowing through the TOE.
	FDP_IFC.1(b)	This requires that the TOE enforce a Diffie-Hellman Information Flow Control Security Functional Policy. The TOE applies administrator-defined firewall rules to the traffic flowing through the TOE. Diffie-Hellman information travels along the same channels as all other information.
	FDP_IFF.1(a)	This defines the subject and information security attributes for the Traffic Information Flow Control Security Functional Policy enforced by the TOE. The traffic firewall rules are defined based on these attributes.
	FDP_IFF.1(b)	This defines the subject and information security attributes for the Diffie-Hellman Information Flow Control Security Functional Policy enforced by the TOE. The Diffie-Hellman traffic firewall rules are defined based on these attributes.
	FDP_ITC.1	This requires that the Diffie-Hellman SFP be enforced when importing the DH public parameter for key exchange. The TOE applies the SFP when Diffie-Hellman traffic enters the TOE.
Identification and Authentication	FIA_UAU.2	This requires that the TSF successfully authenticate administrators before allowing any other actions on behalf of those

		administrators. The TOE checks credentials that individuals attempting to authenticate with the TOE enter and allows access if they are valid.
	FIA_UID.2	This requires that the TSF successfully identify administrators before allowing any other actions on behalf of those administrators. The TOE checks credentials that individuals attempting to authenticate with the TOE enter and allows access if they are valid.
Security Management	FMT_MOF.1	This requires that the ability to modify security functions be restricted to authorized administrators. The TOE provides a graphical interface that authorized administrators can use to manage security functions.
	FMT_MSA.1	This requires that only authorized administrators be allowed to modify the Traffic Information Flow Control SFP. The TOE provides a graphical interface to administrators that only authorized administrators can access.
	FMT_MSA.2	This ensures that only secure values are accepted for security attributes during encryption and decryption. The graphical interface allows administrators to only select secure values for encryption and decryption settings.
	FMT_MSA.3(a)	This requires that the Traffic Information Flow Control SFP provide restrictive default values for security attributes. The TOE blocks all traffic by default.
	FMT_MSA.3(b)	This requires that the Diffie-Hellman Information Flow Control SFP provide permissive default values for security attributes. The TOE allows all Diffie-Hellman attributes to be exchanged by default.
	FMT_SMF.1	This requires that the TSF perform Management of security functions and Management of security attributes. The TOE provides this functionality as described above.

	FMT_SMR.1	This requires that specified roles be maintained by the TOE. The TOE stores roles for all users, and maintains a list of permissions for each of the four roles the TOE can grant.
Protection of the TSF	FPT_RVM.1	This requires that the TSP enforcement functions are invoked and succeed before each function within the TSC is allowed to proceed. The TOE requires a logical flow of data at all times to ensure that security functions occur in the proper order.
	FPT_SEP.1	This requires that the TSF maintain a security domain for its own execution. The TOE does not rely on any other operating system or IT entity to provide it's processing. All security functions are handled by the TOE.
TOE Access	FTA_SSL.3	This requires that the TOE terminate an interactive session after a configurable time interval of administrator inactivity at the Management Console. The TOE drops the connection after this time period expires.

8.7.2 TOE Summary Specification Rationale for the Security Assurance Requirements

EAL 4+ was chosen to provide a basic level of independently assured security in the absence of ready availability of the complete development record from the vendor. The chosen assurance level is consistent with the postulated threat environment.

While the TOE may monitor a hostile environment, it is expected to be in a non-hostile position and embedded in or protected by other products designed to address threats that correspond with the intended environment. The chosen assurance level was also selected for conformance with the client's needs.

8.7.2.1 Configuration Management

The CM documentation provides the description of the Configuration Management System and SonicWALL, Inc.'s CM plan. It describes how the CM system provides automated means to support the generation of the TOE and how automated tools are used in the CM system. A description of tools used to control the configuration items and how they are used at SonicWALL is included. The documentation provides a complete configuration item list and a unique reference for each item. Additionally, the CM system is described including procedures that are used by developers to control and track changes that are made to the TOE. The documentation further details the TOE configuration items that are controlled by the configuration management system.

Corresponding CC Assurance Components:

- Partial CM automation
- Generation support and acceptance procedures
- Problem tracking CM coverage

8.7.2.2 Delivery and Operation

The Delivery and Operation documentation provides a description of the secure delivery procedures implemented by SonicWALL to protect against TOE modification during product delivery. The Installation Documentation provided by SonicWALL details the procedures for installing the TOE and placing the TOE in a secure state offering the same protection properties as the master copy of the TOE. The Installation Documentation provides guidance to the Administrator on the TOE configuration parameters and how they affect the TSF.

Corresponding CC Assurance Components:

- Detection of modification
- Installation, generation, and start-up procedures

8.7.2.3 Development

The SonicWALL design documentation consists of several related design documents that address the components of the TOE at different levels of abstraction. The following design documents address the Development Assurance Requirements:

- The Functional Specification provides a description of the security functions provided by the TOE and a description of the external interfaces to the TSF. The Functional Specification covers the purpose and method of use and a list of effects, exceptions, and errors message for each external TSF interface.
- The High-Level Design provides a top level design specification that refines the TSF functional specification into the major constituent parts (subsystems) of the TSF. The high-level design identifies the basic structure of the TSF, the major elements, a listing of all interfaces, and the purpose, method of use, errors, and exception for each interface.
- The Low-Level Design describes each security supporting module in terms of its purpose and interaction with other modules. It describes the TSF in terms of modules, designating each module as either security-enforcing or security-supporting. It provides an algorithmic description for each security-enforcing module detailed enough to represent the TSF implementation.
- The Implementation Representation unambiguously defines the TSF to a level of detail such that the TSF can be generated without further design decisions. It also describes the relationships between all portions of the implementation.
- The Security Policy Model provides an informal TSP model and it demonstrates correspondence between the functional specification and the TSP model by showing that all of the security functions in the functional specification are consistent and complete with respect to the TSP model. The TSP model describes the rules and characteristics of all policies of the TSP that can be modeled. The model should include a rationale that demonstrates that it is consistent and complete with respect to all policies of the TSP that can be modeled.

- The Correspondence Analysis demonstrates the correspondence between each of the TSF representations provided. This mapping is performed to show the functions traced from all of the adjacent pairs of TSF representation that are provided.

Corresponding CC Assurance Components:

- Fully defined external interfaces
- Security enforcing high-level design
- Subset of the implementation of the TSF
- Descriptive low-level design
- Informal correspondence demonstration
- Informal TOE security policy model

8.7.2.4 Guidance Documentation

The SonicWALL guidance documentation provides guidance on how to securely install and operate the TOE. The guidance provides descriptions of the security functions provided by the TOE. Additionally it provides detailed accurate information on how to administer the TOE in a secure manner and how to effectively use the TSF privileges and protective functions. Since users are not required to interact directly with the TOE, only one set of guidance is provided.

Corresponding CC Assurance Components:

- Administrator guidance
- User guidance

8.7.2.5 Class ALC: Life Cycle Support Documents

The Life Cycle Support documentation describes all the physical, procedural, personnel, and other security measures that are necessary to protect the confidentiality and integrity of the TOE design and implementation in its development environment. It provides evidence that these security measures are followed during the development and maintenance of the TOE. Flaw remediation procedures addressed to TOE developers are provided and so are the established procedures for accepting and acting upon all reports of security flaws and requests for corrections of those flaws. Flaw remediation guidance addressed to TOE users is provided. The description also contains the procedures used by SonicWALL to track all reported security flaws in each release of the TOE. The established life-cycle model to be used in the development and maintenance of the TOE is documented and an explanation of why the model is used is also documented. The selected implementation-dependent options of the development tools are described.

Corresponding CC Assurance Components:

- Identification of security measures
- Developer defined life-cycle model
- Basic flaw remediation
- Well-defined development tools

8.7.2.6 Tests

A number of components make up the Test documentation. The Coverage Analysis demonstrates the testing performed against the functional specification. The Coverage Analysis demonstrates the correspondence between the tests identified in the test documentation and the TSF as described in the functional specification. The depth analysis demonstrates that the tests identified in the test documentation are sufficient to demonstrate that the TSF operates in accordance with its high-level design and low-level design. SonicWALL Test Plans and Test Procedures, which detail the overall efforts of the testing effort and break down the specific steps taken by a tester, are also provided. The Independent Testing documentation provides an equivalent set of resources to those that were used in the developer's functional testing.

Corresponding CC Assurance Components:

- Analysis of coverage
- Testing: high-level design
- Functional testing
- Independent testing – sample

8.7.2.7 Vulnerability and TOE Strength of Function Analyses

The Validation of Analysis documentation identifies all possible modes of operation of the TOE, their consequences and implications for maintaining secure operation. The Strength of TOE Security Function Analysis demonstrates the strength of the probabilistic or permutational mechanisms employed to provide security functions within the TOE and how they exceed the minimum SOF requirements. The Vulnerability Analysis documentation describes the analysis of the TOE deliverables performed to search for ways in which a user can violate the TSP, and the disposition of the identified vulnerabilities.

Corresponding CC Assurance Components:

- Validation of analysis
- Strength of TOE security function evaluation
- Independent vulnerability analysis

8.8 Strength of Function

Strength of function rating of SOF-basic was claimed for this TOE to meet the EAL 4+ assurance requirements. This SOF is sufficient to resist the threats identified in Section 3. Section 4 provides evidence that demonstrates that TOE threats are countered by the TOE security objectives. Section 8 demonstrates that the security objectives for the TOE and the TOE environment are satisfied by the security requirements. The evaluated TOE is intended to operate in commercial and Department of Defense low robustness environments processing unclassified information.

The overall TOE SOF claim is SOF-basic because this SOF is sufficient to resist the threats identified in Section 3.2. Section 8.1 provides evidence that demonstrates that TOE threats are countered by the TOE security objectives. Section 8.2 demonstrates that the security objectives for the TOE and the TOE environment are satisfied by the security requirements.

The relevant security function and security functional requirement which has probabilistic or permutational functions is FIA_UAU.2. The strength of function rating claimed for FIA_UAU.2 is SOF-basic, for the reasons outlined above.

9 Acronyms

Table 22 - Acronyms

Acronym	Definition
3DES	Triple Data Encryption Standard
AES	Advanced Encryption Standard
ARP	Address Resolution Protocol
CA	Certification Authority
CBC	Cipher Block Chaining
CC	Common Criteria for Information Technology Security Evaluation
CEM	Common Evaluation Methodology
CLI	Command Line Interface
CM	Configuration Management
DHCP	Dynamic Host Configuration Protocol
DMZ	Demilitarized Zone
DNS	Dynamic Name System
DPI	Deep Packet Inspection
DSA	Digital Signature Algorithm
EAL	Evaluation Assurance Level
ECB	Electronic Codebook
FIFO	First In/First Out
FIPS	Federal Information Processing Standard
FTP	File Transfer Protocol
GAV	Gateway Antivirus
GMS	Global Management System
GZIP	GNU ZIP
GUI	Graphical User Interface
HMAC	Hashed Message Authentication Code
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol over SSL
ID	Identification
IEC	International Electrotechnical Commission
IKE	Internet Key Exchange
IMAP	Internet Message Access Protocol
IP	Internet Protocol
IPS	Intrusion Prevention System
IPSec	Internet Protocol Security
ISO	International Organization for Standardization

Acronym	Definition
IT	Information Technology
L2	Layer 2
L2TP	Layer 2 Tunneling Protocol
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
LZ77	Lempel-Ziv Coding 1977
MIME	Multipurpose Internet Mail Extensions
NAT	Network Address Translation
NTP	Network Time Protocol
LAN	Local Area Network
POP	Post Office Protocol
PP	Protection Profile
PPPoE	Point to Point over Ethernet
PPTP	Point to Point Tunneling Protocol
PRNG	Pseudo-Random Number Generator
RADIUS	Remote Authentication Dial-In User Service
SA	Security Association
SAR	Security Assurance Requirement
SFP	Security Functional Policy
SFR	Security Functional Requirement
SHA-1	Secure Hashing Algorithm 1
SMTP	Simple Mail Transfer Protocol
SOF	Strength of Function
SPY	Anti-Spyware
SSH	Secure Shell
ST	Security Target
TCP	Transmission Control Protocol
TOE	Target of Evaluation
TSC	TOE Scope of Control
TSF	TOE Security Function
TSP	TOE Security Policy
TSR	Tech Support Report
UDP	User Datagram Protocol
UTM	Unified Threat Management
UUEncode	Unix-to-Unix Encode
VPN	Virtual Private Network
WAN	Wide Area Network

Acronym	Definition
ZIP	Compressed File