Dell SonicWALL, Inc.

SonicOS Enhanced v5.9.0 on NSA Series and TZ Series Appliances

Security Target

Evaluation Assurance Level (EAL): EAL4+
Document Version: 1.1

Prepared for:

Dell SonicWALL, Inc.
2001 Logic Drive
San Jose, CA 95124-3452
United States of America

Phone: +1 888 557 6642
http://www.sonicwall.com

Prepared by:

Corsec Security, Inc.
13135 Lee Jackson Memorial Hwy., Suite 220
Fairfax, VA 22033
United States of America

Phone: +1 703 267 6050
http://www.corsec.com

Table of Contents

© 2014 Dell SonicWALL, Inc.
This document may be freely reproduced and distributed whole and intact including this copyright notice.

Table of Figures

List of Tables

© 2014 Dell SonicWALL, Inc.
This document may be freely reproduced and distributed whole and intact including this copyright notice.

1 Introduction

This section identifies the Security Target (ST), Target of Evaluation (TOE), and the ST organization. The TOE is the SonicWALL SonicOS Enhanced v5.9.0 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. UTMs are consolidated threat-management devices that provide multiple security services, such as network firewall, spam filtering, anti-virus capabilities, intrusion prevention systems (IPS), and World Wide Web content filtering at the network level. SonicWALL appliances also provide Virtual Private Networking (VPN), and traffic management capabilities.

1.1 Purpose

This ST is divided into nine sections, as follows:

- Introduction (Section 1) – Provides a brief summary of the ST contents and describes the organization of other sections within this document. It also provides an overview of the TOE security functions and describes the physical and logical scope for the TOE, as well as the ST and TOE references.
- Conformance Claims (Section 2) – Provides the identification of any Common Criteria (CC), Protection Profile, and Evaluation Assurance Level (EAL) package claims. It also identifies whether the ST contains extended security requirements.
- Security Problem (Section 3) – Describes the threats, organizational security policies, 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.
- Extended Components (Section 5) – Identifies new components (extended Security Functional Requirements (SFRs) and extended Security Assurance Requirements (SARs)) that are not included in CC Part 2 or CC Part 3.
- Security Requirements (Section 6) – Presents the SFRs and SARs met by the TOE.
- TOE Summary Specification (Section 7) – Describes the security functions provided by the TOE that satisfy the security functional requirements and objectives.
- Rationale (Section 8) - Presents the rationale for the security objectives, requirements, and SFR dependencies as to their consistency, completeness, and suitability.
- Acronyms and Terms (Section 9) – Defines the acronyms and terminology used within this ST.

1.2 Security Target and TOE References

Table 1 below shows the ST and TOE references.

Table 1 - ST and TOE References

ST Title	Dell SonicWALL, Inc. SonicOS Enhanced v5.9.0 on NSA Series and TZ Series Appliances Security Target
ST Version	Version 1.1
ST Author	Corsec Security, Inc.
ST Publication Date	2014/2/28
TOE Reference	SonicWALL SonicOS Enhanced v5.9.0.4 build 118 on NSA Series and TZ Series Appliances
FIPS[1] 140-2 Status	Level 2, Validated crypto modules, Certificate No. [TBD]

[1] FIPS – Federal Information Processing Standard

© 2014 Dell SonicWALL, Inc.
This document may be freely reproduced and distributed whole and intact including this copyright notice.

1.3 Product Overview

SonicWALL SonicOS Enhanced v5.9.0 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, IPS, and World Wide Web content filtering[2]. The product under evaluation consists of the SonicOS Enhanced operating system for the following appliances: TZ 105, TZ 105W, TZ 205, TZ 205W, TZ 215, TZ 215W, NSA 220, NSA 220W, NSA 240, NSA 250M, NSA 250MW, NSA 2400, NSA 2400MX, NSA 3500, NSA 4500, NSA E5500, NSA E6500, NSA E7500, NSA E8500, NSA E8510, NSA E10400, NSA E10800, and NSA E10200. The appliances include the same basic functionality, provided by SonicOS Enhanced, but vary in number of processors, size of appliance, and connections they support. These appliances provide firewall, UTM, 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[3].

The SonicOS Enhanced is a proprietary operating system designed for use on SonicWALL appliances. The 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), Application Intelligence and Control, 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 any application layer protocol, encoding, and type of compression. In the event a certain flow of traffic is found to match an Application List signature and meets or exceeds the configured threshold, the event is logged, and the offending flow is terminated.

SonicOS supports VPN functionality[4], which provides a secure connection between two or more computers or protected networks over the public internet. It provides authentication to ensure that 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) version 1 and 2, 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.

[2] Please note that the spam filtering and World Wide Web content filtering functionality is not included as a part of this evaluation.
[3] HTTPS – Hypertext Transfer Protocol over Secure Sockets Layer (SSL)
[4] For use with SonicWALL Global VPN Client and GroupVPN. These are other SonicWALL products that are not a part of this evaluation.

© 2014 Dell SonicWALL, Inc.
This document may be freely reproduced and distributed whole and intact including this copyright notice.

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 Wide Area Network (WAN) interfaces through Dynamic Host Configuration Protocol (DHCP), Point to Point Protocol 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 and virtual Multicast), 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.
- 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. The System Time will be set to no automatically update using NTP for the evaluation.

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

- Dashboard: The Visualization Dashboard allows administrators to monitor the network, logs, connections, and applications.

© 2014 Dell SonicWALL, Inc.
This document may be freely reproduced and distributed whole and intact including this copyright notice.

- System: Security appliance controls such as managing system status, managing licenses, configuring remote management options, managing firmware versions and preferences, and troubleshooting diagnostic tools.
- Network: Configure logical interfaces, load balancing, failover, security zones, address objects, routing, the DHCP server, IP Helper, web proxy server, and dynamic DNS. Creation of NAT policies and setting up DNS servers is also available.
- Third Generation (3G)/Analog Modem, Wireless, and SonicPoint: Different pages on wireless functionality, which is excluded from the TOE.
- Firewall and Firewall Settings: Establish access rules.
- DPI-SSL: Allows DPI of encrypted HTTPS traffic. This functionality is not included in the evaluation.
- Voice over IP (VoIP): Setup and configuration of Session Initiated Protocol (SIP) Voice over IP using IPSec VPNs.
- Anti-Spam: Configuring the anti-spam feature.
- VPN: Creating VPN policies and creating site-to-site VPN policies
- User Management: Configure appliances for user level authentication.
- High Availability: Configure high availability settings.
- Security Services: Activating security services and use of Intrusion Protection Service, Content Filtering, and Client Anti-Virus.
- Log: Managing the logs and alerts for the system.

Event logging by SonicOS provides a mechanism for tracking potential security threats. Administrators can view and sort the log via the Web Management Interface, 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 four modes of operation: Layer 2 Bridged Mode, Transparent Mode, IPS Sniffer Mode, and Wire 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.

Each appliance includes a cryptographic module that the TOE relies upon. This cryptographic module has been FIPS 140-2 validated by NIST[5] and CSE[6], Certificate No: TBD. The appliance and its cryptographic module are outside the TOE scope, and therefore its internals are not covered by this evaluation.

1.4 TOE Overview

The TOE Overview summarizes the usage and major security features of the TOE. The TOE Overview provides a context for the TOE evaluation by identifying the TOE type, describing the product, and defining the specific evaluated configuration.

The TOE is a firewall/UTM/VPN that runs on a TZ 105, TZ 105W, TZ 205, TZ 205W, TZ 215, TZ 215W, NSA 220, NSA 220W, NSA 240, NSA 250M, NSA 250MW, NSA 2400, NSA 2400MX, NSA 3500, NSA

[5] NIST – National Institute of Standards and Technology
[6] CSE – Communications Security Establishment Canada

© 2014 Dell SonicWALL, Inc.
This document may be freely reproduced and distributed whole and intact including this copyright notice.

4500, NSA E5500, NSA E6500, NSA E7500, NSA E8500, NSA E8510, NSA E10400, NSA E10800, and NSA E10200 SonicWALL appliance. The appliance is installed on a network wherever firewall/UTM/VPN services are required, as depicted in Figure 1 below. This may be used at the edge of a network for perimeter security or between different segments of a network for internal security. The TOE is software only with the hardware listed above as part of the TOE environment.

The TOE includes all of the components and functionality described above in section 1.3 and below in section 1.5, except for the features and functionality listed below in section 1.5.3. Table 2 identifies any major non-TOE hardware and software that is required by the TOE including the TOE minimum requirements.

Figure 1 shows the details of the basic deployment configuration of the TOE:

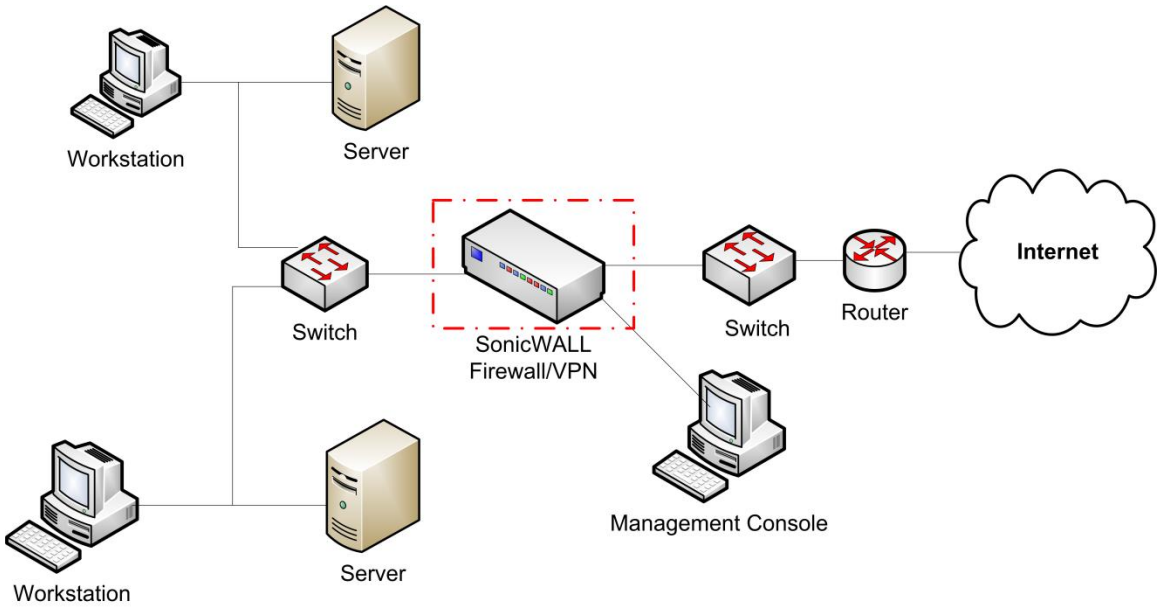

Figure 1 – Basic Deployment Configuration of the TOE

The TOE may be deployed with another instance of the TOE to provide a VPN between two sites. Figure 2 depicts this type of deployment.

© 2014 Dell SonicWALL, Inc.
This document may be freely reproduced and distributed whole and intact including this copyright notice.

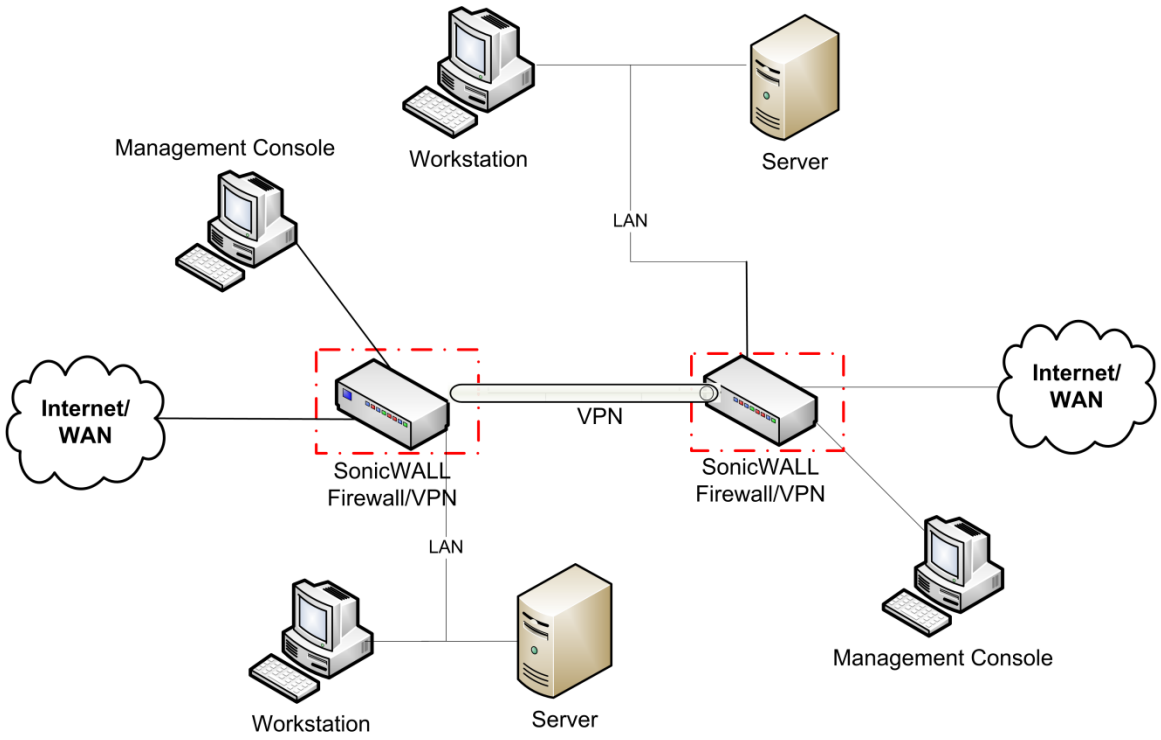

Figure 2 – VPN Deployment Configuration of the TOE

1.4.1 TOE Environment

The TOE environment consists of the SonicWALL hardware for the appliances listed below in Table 2, and a management console for managing the TOE. The environment also includes a hardware accelerator chip that can be used for speeding up encryption and decryption functions. Table 2 specifies the minimum system requirements for the proper operation of the TOE.

Table 2 - TOE Minimum Requirements

Category	Requirement
NSA Appliances	220, 220W, 240, 250M, 250MW, 2400, 2400MX, 3500, 4500, E5500, E6500, E7500, E8500, E8510, E10400, E10800, and E10200
TZ Appliances	105, 105W, 205, 205W, 215, and 215W
Management Console	General purpose computer with: • Chrome 4.0 and higher (recommended browser) • Mozilla 3.0 and higher • Internet Explorer 8.0 and higher for HTTPS management sessions.

In addition, the TOE needs cable and connectors that allow all of the TOE and environmental components to communicate with each other.

1.5 TOE Description

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

© 2014 Dell SonicWALL, Inc.
This document may be freely reproduced and distributed whole and intact including this copyright notice.

1.5.1 Physical Scope

Figure 3 illustrates the physical scope and the physical boundary of the overall solution and ties together all of the components of the TOE.

The TOE is a UTM which runs on the SonicWALL NSA series and TZ series hardware appliances listed in Table 2. The TOE is installed on a network wherever firewall/UTM/VPN services are required, as depicted in the figure below. The essential physical components for the proper operation of the TOE in the evaluated configuration are

- SonicOS Enhanced

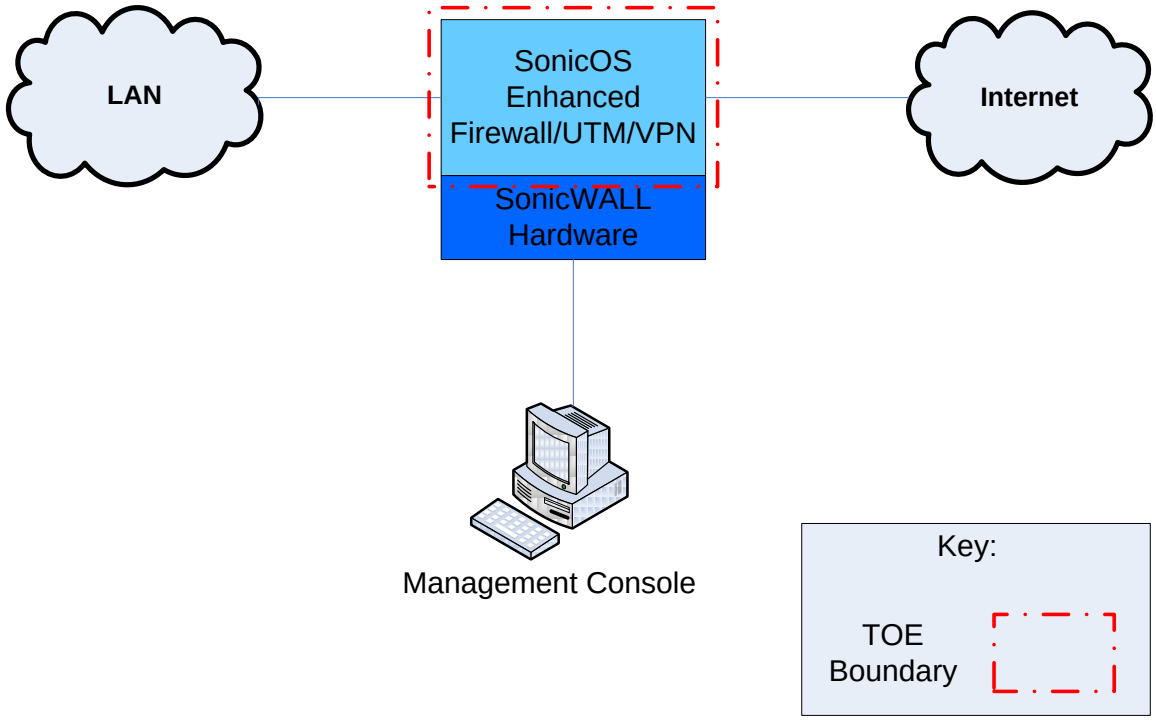

Figure 3 - Physical TOE Boundary

1.5.1.1 TOE Firmware

The TOE is the operating system that runs the Firewall/UTM/VPN appliance.

1.5.1.2 Guidance Documentation

The following guides are required reading and part of the TOE:

- Dell SonicWALL SonicOS Enhanced 5.9 Administrator's Guide
- Dell SonicWALL SonicOS 5.9.1.0 Release Notes
- Dell SonicWALL SonicOS 5.9.1 Log Event Reference
- One of the following, based on the appliance used:
  - Dell SonicWALL NSA 220 Quick Start Poster
  - Dell SonicWALL NSA 240 Getting Started Guide
  - Dell SonicWALL NSA 250M or 250 MW Quick Start Poster
  - Dell SonicWALL NSA 2400 Getting Started Guide
  - Dell SonicWALL NSA 2400MX Getting Started Guide

© 2014 Dell SonicWALL, Inc.
This document may be freely reproduced and distributed whole and intact including this copyright notice.

- Dell SonicWALL NSA 5000/4500/3500 Getting Started Guide
- Dell SonicWALL NSA E5500 Getting Started Guide
- Dell SonicWALL NSA E6500 Getting Started Guide
- Dell SonicWALL NSA E7500 Getting Started Guide
- Dell SonicWALL NSA E8500 Getting Started Guide
- Dell SonicWALL NSA E8510 Getting Started Guide
- Dell SonicWALL TZ 105 Quick Start Poster
- Dell SonicWALL TZ 205 Quick Start Poster
- Dell SonicWALL TZ 215 Quick Start Poster
- Dell SonicWALL SuperMassive Series Datasheet

The NSA E10200, E10400, and E10800 are installed by SonicWALL professional services and therefore do not have an associated Getting Started Guide or Poster.

1.5.2 Logical Scope

The logical boundary of the TOE will be broken down into the following security classes which are further described in sections 6 and 7 of this ST. The logical scope also provides the description of the security features of the TOE. 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 TOE Security Function (TSF)
- TOE Access

1.5.2.1 Security Audit

The TOE generates audit records for startup and shutdown of the audit functions, blocked traffic, blocked websites, administrator account activity, VPN activity, firewall activity, firewall rule modification, network access, IPS/GAV/SPY activity, and login attempts. Administrators can view, search, sort and order the audit records based on priority, category, source IP or Interface, and destination IP or interface.

1.5.2.2 Cryptographic Support

The TOE provides IPSec VPN functionality for secure communications over the public internet. IKE protocol is used for exchanging authentication information and establishing the VPN tunnel. The TOE supports both version 1 and version 2 of IKE. The TOE is only installed and run on SonicWALL appliances that are validated to FIPS 140-2, all cryptographic operations are performed in accordance with FIPS 140-2, and all keys, algorithms, and key destruction meet the FIPS 140-2 standard. The cryptographic internals are not included in the evaluation and are part of the TOE's operational environment. The TOE uses the SonicOS Cryptography module's interface to request and receive cryptographic services.

1.5.2.3 User Data Protection

The TOE controls network traffic via the Traffic Information Flow Control Security Functional Policy (SFP). The Traffic Information Flow SFP relies on source and destination IP addresses, protocol type, port numbers, port types or subtypes, and rules defined in the Traffic Information Flow Control Lists to determine how to treat the network traffic. The rules define external IT entities that send traffic through the TOE as subjects and the traffic sent by these subjects as the information. These rules determine whether traffic should be passed through the TOE to its destination, be denied passage through the network, or be discarded. Keys and key parameters destined for the TOE are allowed and imported without security attributes associated.

© 2014 Dell SonicWALL, Inc.
This document may be freely reproduced and distributed whole and intact including this copyright notice.

VPN traffic follows the VPN Information Flow Control SFP. As traffic enters the TOE, the packet headers are checked to determine protocol type. If the packet header includes an IPsec header the traffic is allowed and decrypted. If the header does not include an IPsec header the Traffic Information Flow Control Policy SFP is enforced. The VPN Flow Control SFP defines subjects as users of the VPN tunnel and the information as the traffic these subjects send through the tunnel in encrypted form.

1.5.2.4 Identification and Authentication

Administrators are required to successfully identify and authenticate with the TOE prior to any actions on the TOE. Username, password, and role are stored in the TOE and are compared against the username and password entered by an administrator before assigning a role and allowing access.

1.5.2.5 Security Management

Table 12 lists the management security functions for the TOE and the operations each role can perform. The TOE supports the roles of Full Administrator, Limited Administrator, and Read-Only Administrator. The Full and Limited Administrators have different permission based on if they are in configuration mode or not. When these administrators are in configuration mode they are called Config Mode Full Administrators and Config Mode Limited Administrators. The Config Mode Full Administrator role has the ability to modify and delete the restrictive default security attributes for the Traffic and Information Flow Control SFP. The TOE ensures that only secure values of the security attributes are accepted. The VPN Flow Control SFP security attributes have restrictive default values that cannot be changed.

1.5.2.6 Protection of the TSF

The TSF provides a reliable timestamp for operations in the TOE.

1.5.2.7 TOE Access

An administrator can configure the TOE to terminate management sessions after five to 60 minutes of inactivity. The default time for termination is 15 minutes.

1.5.3 Product Physical/Logical Features and Functionality not included in the TSF

Features/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 (Simple Mail Transfer Protocol (SMTP))
- Global Security Client (including GroupVPN)
- Global Management System (GMS)
- SonicPoint
- VoIP

© 2014 Dell SonicWALL, Inc.
This document may be freely reproduced and distributed whole and intact including this copyright notice.

2 Conformance Claims

This section and Table 3 provide the identification for any CC, Protection Profile (PP), and EAL package conformance claims. Rationale is provided for any extensions or augmentations to the conformance claims. Rationale for CC and PP conformance claims can be found in Section 8.1.

Table 3 - CC and PP Conformance

Common Criteria (CC) Identification and Conformance	Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 4, September 2012; CC Part 2 conformant; CC Part 3 conformant; PP claim (none); Parts 2 and 3 Interpretations of the CEM as of 2014/2/28 were reviewed, and no interpretations apply to the claims made in this ST.
PP Identification	None
Evaluation Assurance Level	EAL4+ augmented with Flaw Remediation ALC_FLR.2

© 2014 Dell SonicWALL, Inc.
This document may be freely reproduced and distributed whole and intact including this copyright notice.

3 Security Problem

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:

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

3.1 Threats to Security

This section identifies the threats to the IT[7] 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 users: They have public knowledge of how the TOE operates and are assumed to possess an enhanced basic skill level, limited resources to alter TOE configuration settings or parameters and no physical access to the TOE.
- TOE users: 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 or parameters and physical access to the TOE. (TOE users 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 TSF and 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. Table 4 below lists the applicable threats.

Table 4 - 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.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.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.MEDIAT	An unauthorized person may send impermissible information through the TOE which results in the exploitation of resources on the internal network.

[7] IT – Information Technology

© 2014 Dell SonicWALL, Inc.
This document may be freely reproduced and distributed whole and intact including this copyright notice.

Name	Description
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.

3.2 Organizational Security Policies

This Security Target defines no Organizational Security Policies.

3.3 Assumptions

This section 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. Table 5 lists the specific conditions that are required to ensure the security of the TOE and are assumed to exist in an environment where this TOE is employed.

Table 5 - Assumptions

Name	Description
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 moderate.
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.NOEVIL	Authorized administrators are non-hostile and follow all administrator guidance.
A.REMACC	Authorized administrators may only access the TOE locally.
A.UPS	The TOE will be supported by an Uninterruptible Power Supply.
A.FIPS	The TOE will only be installed and run on SonicWALL appliances that have been evaluated under FIPS 140-2 with the same version of the TOE.

© 2014 Dell SonicWALL, Inc.
This document may be freely reproduced and distributed whole and intact including this copyright notice.

4 Security Objectives

Security objectives are concise, abstract statements of the intended solution to the problem defined by the security problem definition (see Section 3). The set of security objectives for a TOE form a high-level solution to the security problem. This high-level solution is divided into two part-wise solutions: the security objectives for the TOE, and the security objectives for the TOE's operational environment. This section identifies the security objectives for the TOE and its supporting environment.

4.1 Security Objectives for the TOE

The specific security objectives for the TOE are listed in Table 6 below.

Table 6 - Security Objectives for the TOE

Name	Description
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.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.AUTHENTICATE	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.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.MEDIATE	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.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.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 and read, modify, or destroy configuration data.
O.TIME	The TOE provides a reliable time stamp.
O.VPN	The TOE must be able to protect the integrity and confidentiality of data transmitted to a peer authorized external IT entity via requests for encryption and authentication for such data. Upon receipt of data from a peer authorized external IT entity, the TOE must be able to request decryption of the data and verify that the received data accurately represents the data that was originally transmitted.

© 2014 Dell SonicWALL, Inc.
This document may be freely reproduced and distributed whole and intact including this copyright notice.

4.2 Security Objectives for the Operational Environment

This section describes the environmental objectives.

4.2.1 IT Security Objectives

Table 7 below lists the IT security objectives that are to be satisfied by the environment.

Table 7 - IT Security Objectives

Name	Description
OE.VPN	The TOE Environment must be able to provide cryptographic services as requested by the TOE. These cryptographic services are provided from the operational environment's validated cryptographic services only.

4.2.2 Non-IT Security Objectives

Table 8 below lists the non-IT environment security objectives that 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 8 - Non-IT Security Objectives

Name	Description
NOE.DIRECT	The TOE is available to authorized administrator only.
NOE.FIPS	The TOE will only be installed and run on SonicWALL appliances that have been evaluated under FIPS 140-2 with the same version of the TOE.
NOE.GENPUR	The TOE only stores and executes security-relevant applications and only stores data required for its secure operation.
NOE.MODEXP	The threat of malicious attacks aimed at discovering exploitable vulnerabilities is considered moderate.
NOE.NOEVIL	Authorized administrators are non-hostile and follow all administrator guidance.
NOE.PHYSEC	The physical environment must be suitable for supporting a computing device in a secure setting.
NOE.PUBLIC	The TOE does not host public data.
NOE.REMACC	Authorized administrators may only access the TOE locally.
NOE.SINGEN	Information cannot flow among the internal and external networks unless it passes through the TOE.
NOE.UPS	The TOE will be supported by an Uninterruptible Power Supply.

© 2014 Dell SonicWALL, Inc.
This document may be freely reproduced and distributed whole and intact including this copyright notice.

5 Extended Components

This section defines the extended SFRs and extended SARs met by the TOE. These requirements are presented following the conventions identified in Section 6.1.

5.1 Extended TOE Security Functional Components

There are no extended SFRs for the TOE.

5.2 Extended TOE Security Assurance Components

There are no the extended SARs for the TOE.

© 2014 Dell SonicWALL, Inc.
This document may be freely reproduced and distributed whole and intact including this copyright notice.

6 Security Requirements

This section defines the SFRs and SARs met by the TOE. These requirements are presented following the conventions identified in Section 6.1.

6.1 Conventions

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

The 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 Part 2 of the CC, and are shown as follows:

- Completed assignment statements are identified using [*italicized text within brackets*].
- Completed selection statements are identified using [underlined text within brackets].
- Refinements are identified using **bold text**. Any text removed is stricken (Example: ~~TSF Data~~) and should be considered as a refinement.
- Extended Functional and Assurance Requirements are identified using "EXT_" at the beginning of the short name.
- 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.

6.2 Security Functional Requirements

This section specifies the SFRs for the TOE. This section organizes the SFRs by CC class. Table 9 identifies all SFRs implemented by the TOE and indicates the ST operations performed on each requirement.

Table 9 - 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	✓	✓		
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			✓	

© 2014 Dell SonicWALL, Inc.
This document may be freely reproduced and distributed whole and intact including this copyright notice.

Name	Description	S	A	R	I
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_STM.1	Reliable time stamps				
FTA_SSL.3	TSF-initiated termination		✓		

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

© 2014 Dell SonicWALL, Inc.
This document may be freely reproduced and distributed whole and intact including this copyright notice.

6.2.1 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 (if applicable), and the outcome (success or failure) of the event; and

b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [*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 apply [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

© 2014 Dell SonicWALL, Inc.
This document may be freely reproduced and distributed whole and intact including this copyright notice.

6.2.2 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 10*] and specified cryptographic key sizes [*cryptographic key sizes – see Table 10*] that meet the following: [*list of standards – see Table 10*].

Table 10 – Cryptographic Key Generation Standards

Key Generation Type	Algorithm and Key Sizes	Standards (Certificate #)
DRBG[8]	Hash-based DRBG –256 bit	SP 800-90A (certificate 189)
Diffie-Hellman key agreement	Diffie-Hellman 1024 bit	RFC 2631 SP800-56A

Dependencies: FCS_COP.1 Cryptographic operation,
FCS_CKM.4 Cryptographic key destruction

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: FCS_CKM.1 Cryptographic key generation

FCS_COP.1 Cryptographic operation
Hierarchical to: No other components.
FCS_COP.1.1

The TSF shall perform [*list of cryptographic operations – see Table 11*] in accordance with a specified cryptographic algorithm [*cryptographic algorithm – see Table 11*] and cryptographic key sizes [*cryptographic key sizes – see Table 11*] that meet the following: [*list of standards – see Table 11*].

Table 11 – Cryptographic Operations

Cryptographic Operations	Cryptographic Algorithm	Key Sizes (bits)	Standards (Certificate #)
Digital signature verification (legacy-use only)	RSASSA-PKCS1-v1.5	1024, 1536	FIPS 186-3 (certificates #1044)

[8] DRBG – Deterministic Random Bit Generator

© 2014 Dell SonicWALL, Inc.
This document may be freely reproduced and distributed whole and intact including this copyright notice.

Cryptographic Operations	Cryptographic Algorithm	Key Sizes (bits)	Standards (Certificate #)
Digital signature verification	RSASSA-PKCS1-v1.5	2048	FIPS 186-3 (certificate #1044)
Digital signature generation	RSASSA-PKCS1-v1.5	2048	FIPS 186-3 (certificate #1044)
Symmetric encryption and decryption	Advanced Encryption Standard (AES) (CBC[9] mode)	128, 192, 256	FIPS 197 (certificates #2015)
	Triple-Data Encryption Standard (3DES) (TCBC[10] mode)(3 key)	168[11]	NIST SP 800-67, May 2008 (certificates #1300)
Hashing	Secure Hash Algorithm1 (SHA -1), SHA-256, SHA-384, SHA-512	Not Applicable	FIPS 180-2 (certificates #1765)
Message Authentication	Keyed-Hash Message Authentication Code (HMAC) with Secure Hash 256 (SHA -256)	256	FIPS 198 (certificates #1219)

Dependencies: **FCS_CKM.1 Cryptographic key generation**
FCS_CKM.4 Cryptographic key destruction

[9] CBC – Cipher Block Chaining mode
[10] TCBC – Triple DES Cipher Block Chaining mode
[11] Although the key size is 168 bits, the assessed key strength is only 112 bits per SP 800-131A.

© 2014 Dell SonicWALL, Inc.
This document may be freely reproduced and distributed whole and intact including this copyright notice.

6.2.3 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*] 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(a) 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 [*VPN Information Flow Control SFP*] on [
a) SUBJECTS: VPN users,
b) INFORMATION: VPN traffic, and
c) OPERATIONS: ALLOW and decrypt or enforce Traffic Information Flow Control].
Dependencies: FDP_IFF.1(b) Simple security attributes

FDP_IFF.1(a) Simple security attributes
Hierarchical to: No other components.
FDP_IFF.1.1(a)
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) 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 explicitly authorise an information flow based on the following rules: [*no other rules*].
FDP_IFF.1.5(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

© 2014 Dell SonicWALL, Inc.
This document may be freely reproduced and distributed whole and intact including this copyright notice.

Hierarchical to: No other components.

FDP_IFF.1.1(b)

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

SUBJECT (VPN users) attributes:

1) IP address, and

INFORMATION (VPN traffic) attributes:

1) Protocol type

2) IPsec header].

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: [*a VPN policy has been established between two instance of the TOE and the packets have a valid IPsec header indicating IPsec protocol type*].

FDP_IFF.1.3(b)

The TSF shall enforce the [*Traffic Information Flow Control SFP if no IPsec header exists*].

FDP_IFF.1.4

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

FDP_IFF.1.5(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 [*Traffic Information Flow Control SFP*] when importing user data, controlled under the SFP, from outside the TOE.

FDP_ITC.1.2

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

FDP_ITC.1.3

The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TOE: [

1. *Keys and key parameters that are imported from outside the TOE as part of the VPN tunnel setup are always assigned an ALLOW operation*
2. *all other user data passing through the TOE are subject to the rules defined in the Traffic Information Flow Control SFP*].

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

© 2014 Dell SonicWALL, Inc.
This document may be freely reproduced and distributed whole and intact including this copyright notice.

6.2.4 Class FIA: Identification and Authentication

FIA_UAU.2 User authentication before any action
Hierarchical to: FIA_UAU.1 Timing of authentication
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 Timing of identification
FIA_UID.2.1
The TSF shall require each ~~user~~ **administrator** to be successfully identified before allowing any other TSF-mediated actions on behalf of that ~~user~~ **administrator**.
Dependencies: No dependencies

© 2014 Dell SonicWALL, Inc.
This document may be freely reproduced and distributed whole and intact including this copyright notice.

6.2.5 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 actions in the action column of Table 12 below] the functions [*specified in Table 12 below*] to [*the roles and mode as specified in Table 12 below*].

Table 12 – Management of Security Functions Behavior

Roles / Action	Config Mode Full Administrator	Non-Config Mode Full Administrator	Read-Only Administrator	Config Mode Limited Administrator	Non-Config Mode Limited Administrator
determine the behaviour of	interface settings, zones, DNS settings, address objects, NAT policies, and DHCP server settings	interface settings, DNS settings, address objects, NAT policies, and DHCP server settings	interface settings, DNS settings, address objects, NAT policies, and DHCP server settings	interface settings and DNS settings	interface settings and DNS settings
disable	VPN Policies	none	none	none	none
enable	VPN Policies, firmware settings, ARP cache flush	ARP cache flush	none	ARP cache flush	ARP cache flush
modify the behaviour of	configure interface settings, zones, DNS settings, address objects, NAT policies, and configure DHCP server	none	none	configure interface settings and DNS settings	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 [[*delete from and add to 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 [*Config Mode Full Administrator role*].

Dependencies: FDP_IFC.1(a) 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

© 2014 Dell SonicWALL, Inc.
This document may be freely reproduced and distributed whole and intact including this copyright notice.

The TSF shall ensure that only secure values are accepted for [*Source IP address, Destination IP address, Protocol Type, port number, port type or subtype*].

Dependencies: **FDP_IFC.1(a) 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

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

The TSF shall allow the [*Config Mode Full Administrator 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

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

FMT_MSA.3.2

The TSF shall allow the [*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 management functions: [*certificates, firmware settings, running diagnostics and creating tech support requests, log off other users, unlock users, log management, and management of flow control 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, Limited Administrator, and Read-Only Administrator*].

FMT_SMR.1.2

The TSF shall be able to associate users with roles.

Dependencies: **FIA_UID.1 Timing of identification**

© 2014 Dell SonicWALL, Inc.
This document may be freely reproduced and distributed whole and intact including this copyright notice.

6.2.6 Class FPT: Protection of the TSF

FPT_STM.1 Reliable Timestamp
Hierarchical to: No other components.
FPT_STM.1.1
The TSF shall be able to provide reliable time stamps.
Dependencies: No Dependencies

© 2014 Dell SonicWALL, Inc.
This document may be freely reproduced and distributed whole and intact including this copyright notice.

6.2.7 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

© 2014 Dell SonicWALL, Inc.
This document may be freely reproduced and distributed whole and intact including this copyright notice.

6.3 Security 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.2. Table 13 - Assurance Requirements summarizes the requirements.

Table 13 - Assurance Requirements

Assurance Requirements	
Class ASE: Security Target evaluation	ASE_CCL.1 Conformance claims
	ASE_ECD.1 Extended components definition
	ASE_INT.1 ST introduction
	ASE_OBJ.2 Security objectives
	ASE_REQ.2 Derived security requirements
	ASE_SPD.1 Security problem definition
	ASE_TSS.1 TOE summary specification
Class ALC : Life Cycle Support	ALC_CMC.4 Production support, acceptance procedures and automation
	ALC_CMS.4 Problem tracking CM Coverage
	ALC_DEL.1 Delivery Procedures
	ALC_DVS.1 Identification of security measures
	ALC_LCD.1 Developer defined life-cycle model
	ALC_TAT.1 Well-defined development tools
	ALC_FLR.2 Flaw reporting procedures
Class ADV: Development	ADV_ARC.1 Security Architecture Description
	ADV_FSP.4 Complete functional specification
	ADV_IMP.1 Implementation representation of the TSF
	ADV_TDS.3 Basic modular design
Class AGD: Guidance documents	AGD_OPE.1 Operational user guidance
	AGD_PRE.1 Preparative procedures
Class ATE: Tests	ATE_COV.2 Analysis of coverage
	ATE_DPT.1 Testing: basic design
	ATE_FUN.1 Functional testing
	ATE_IND.2 Independent testing – sample
Class AVA: Vulnerability assessment	AVA_VAN.3 Focused Vulnerability analysis

© 2014 Dell SonicWALL, Inc.
This document may be freely reproduced and distributed whole and intact including this copyright notice.

7 TOE Summary Specification

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

7.1 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 14 lists the security functions and their associated SFRs.

Table 14 - 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
Cryptographic Support	FCS_CKM.1	Cryptographic key generation
	FCS_CKM.4	Cryptographic key destruction
	FCS_COP.1	Cryptographic operation
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
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_STM.1	Reliable time stamps

© 2014 Dell SonicWALL, Inc.
This document may be freely reproduced and distributed whole and intact including this copyright notice.

TOE Security Function	SFR ID	Description
TOE Access	FTA_SSL.3	TSF-initiated termination

7.1.1 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 15 below.

The TOE audit records contain the following information:

Table 15 - 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
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.

7.1.2 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 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

© 2014 Dell SonicWALL, Inc.
This document may be freely reproduced and distributed whole and intact including this copyright notice.

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. The TOE uses the SonicOS Cryptographic module's interfaces to request and receive all cryptographic operations.

Encryption methods implemented by the TOE include three key 3DES, AES-128, AES-192, and AES-256. The hashing methods used to sign the key include HMAC, SHA-1, and SHA-256. RSA 1024 and 1536 are used only for legacy-use in digital signature verification. SHA-1 is used for legacy-use digital signature verification and for hash-only applications. Digital signatures are only generated using RSA 2046 and SHA-256 or higher. 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.

7.1.3 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 VPN Information Flow Control SFP distinguishes VPN packets from other packets based on the packet headers. If a packet header has a valid IPsec header it is allowed and decrypted. If a packet header does not have a valid IPsec header the Traffic Information Flow Control SFP is enforced. The Traffic 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. Keys or key parameters that are sent to the TOE are imported without security attributes associated and are allowed per the Traffic Information Flow Control SFP.
TOE Security Functional Requirements Satisfied: FDP_IFC.1(a), FDP_IFC.1(b), FDP_IFF.1(a), FDP_IFF.1(b), FDP_ITC.1.

7.1.4 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 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.

© 2014 Dell SonicWALL, Inc.
This document may be freely reproduced and distributed whole and intact including this copyright notice.

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

7.1.5 Security Management

The Security Management function specifies the management of several aspects of the TSF, including security function behavior and security attributes. The various management roles are also specified here: Full Administrator, Limited Administrator, and Read-Only Administrator. Each role enforced by this TSF has different privileges to access and configure the behavior of the TOE. Full Administrators and Limited Administrators must enter configuration mode to perform certain functions. Only one administrator can be in configuration mode at a time. The roles are referred to as Config Mode Full Administrators and Non-Config Mode Full Administrator to specify the role and its mode. For example, Config Mode Full Administrator roles can perform any configuration of the TOE, whereas Config Mode Limited Administrator role 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 Traffic Information Flow Control SFP is limited to administrators with the role Config Mode Full Administrator. Also, specifying alternative initial values for security attributes to override the default values is limited to administrators with the role Config Mode Full Administrator. These values are checked by the TSF to ensure that only secure values are accepted.

The IPsec header and protocol type of VPN traffic are set to restrictive default values since the header does not exist unless the traffic is part of a valid VPN policy. These values cannot be changed by any role in the TSF.
TOE Security Functional Requirements Satisfied: FMT_MOF.1, MFT_MSA.1, FMT_MSA.3, FMT_SMF.1, FMT_SMR.1.

7.1.6 Protection of the TSF

The TOE maintains a reliable timestamp for audit messages.
TOE Security Functional Requirements Satisfied: FPT_STM.1.

7.1.7 TOE Access

The TOE Access function specifies requirements for controlling the establishment of an administrator's session. The TSF provides this function by terminating a management session after a configurable time interval of administrator inactivity at the Web Management Interface. The default time interval is 5 minutes. This can be configured by an administrator to an interval between one 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.

© 2014 Dell SonicWALL, Inc.
This document may be freely reproduced and distributed whole and intact including this copyright notice.

8 Rationale

8.1 Conformance Claims Rationale

This Security Target conforms to Part 2 and Part 3 of the *Common Criteria for Information Technology Security Evaluation*, Version 3.1 Revision 3.

8.2 Security Objectives Rationale

This section provides a rationale for the existence of each threat, policy statement, and assumption that compose the Security Target. Sections 8.2.1, 8.2.2, and 8.2.3 demonstrate the mappings between the threats, policies, and assumptions to the security objectives are complete. The following discussion provides detailed evidence of coverage for each threat, policy, and assumption.

8.2.1 Security Objectives Rationale Relating to Threats

Table 16 below provides a mapping of the objects to the threats they counter.

Table 16 – Threats:Objectives Mapping

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.MEDIATE 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.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.
	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.TIME The TOE provides a reliable time stamp.	The O.TIME objective addresses the T.AUDACC threat by requiring the TOE to provide reliable timestamps for use in audit records. Authorized administrators may use the audit records to identify attacker actions.

© 2014 Dell SonicWALL, Inc.
This document may be freely reproduced and distributed whole and intact including this copyright notice.

Threats	Objectives	Rationale
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.AUTHENTICATE 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.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.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.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 functionality.
	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 and read, modify, or destroy configuration data.	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.VPN The TOE must be able to protect the integrity and confidentiality of data transmitted to a peer authorized external IT entity via requests for encryption and authentication for such data. Upon receipt of data from a peer authorized external IT entity, the TOE must be able to request	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.

© 2014 Dell SonicWALL, Inc.
This document may be freely reproduced and distributed whole and intact including this copyright notice.

Threats	Objectives	Rationale
	decryption of the data and verify that the received data accurately represents the data that was originally transmitted.	
	OE.VPN The TOE Environment must be able to provide cryptographic services as requested by the TOE. These cryptographic services are provided from the operational environment's validated cryptographic services only.	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.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 and read, modify, or destroy configuration data.	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.MEDIAT An unauthorized person may send impermissible information through the TOE which results in the exploitation of resources on the internal network.	O.MEDIATE The TOE must mediate the flow of all information between clients and servers located on internal and external networks governed by the TOE, 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 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.

© 2014 Dell SonicWALL, Inc.
This document may be freely reproduced and distributed whole and intact including this copyright notice.

Threats	Objectives	Rationale
	O.SELPRO The TOE must protect itself against attempts by unauthorized users to bypass, deactivate, or tamper with TOE security functions and read, modify, or destroy configuration data.	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.
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 requests for encryption and authentication for such data. Upon receipt of data from a peer authorized external IT entity, the TOE must be able to request decryption of 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 provide cryptographic services as requested by the TOE. These cryptographic services are provided from the operational environment's validated cryptographic services only.	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 requests for encryption and authentication for such data. Upon receipt of data from a peer authorized external IT entity, the TOE must be able to request decryption of 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 provide cryptographic services as requested by the TOE. These cryptographic services are provided from the operational	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

© 2014 Dell SonicWALL, Inc.
This document may be freely reproduced and distributed whole and intact including this copyright notice.

Threats	Objectives	Rationale
	environment's validated cryptographic services only.	external IT entity via encryption and provides authentication for such data.

Every Threat is mapped to one or more Objectives in the table above. This complete mapping demonstrates that the defined security objectives counter all defined threats.

8.2.2 Security Objectives Rationale Relating to Policies

There are no organizational security policies defined for this ST.

8.2.3 Security Objectives Rationale Relating to Assumptions

Table 17 below gives a mapping of assumptions and the environmental objectives that uphold them.

Table 17 – Assumptions:Objectives Mapping

Assumptions	Objectives	Rationale
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 administrator 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 physical environment must be suitable for supporting a computing device in a secure setting.	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 moderate.	NOE.MODEXP The threat of malicious attacks aimed at discovering exploitable vulnerabilities is considered moderate.	The NOE.MODEXP objective ensures that the threat of malicious attacks aimed at discovering exploitable vulnerabilities is moderate.
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 Information cannot flow among the internal and external networks unless it passes through the TOE.	NOE.SINGEN Information cannot flow among the internal and external networks unless it passes through the TOE.	The NOE.SINGEN objective ensures that information cannot flow among the internal and external networks unless it passes through the TOE.
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.

© 2014 Dell SonicWALL, Inc.
This document may be freely reproduced and distributed whole and intact including this copyright notice.

Assumptions	Objectives	Rationale
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.FIPS The TOE will only be installed and run on SonicWALL appliances that have been evaluated under 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 evaluated under 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 evaluated under FIPS 140-2 on the same version of the TOE.

Every assumption is mapped to one or more Objectives in the table above. This complete mapping demonstrates that the defined security objectives uphold all defined assumptions.

8.3 Rationale for Extended Security Functional Requirements

There are no extended security functional requirements defined for this ST.

8.4 Rationale for Extended TOE Security Assurance Requirements

There are no extended TOE security assurance requirements defined for this ST.

8.5 Security Requirements Rationale

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

8.5.1 Rationale for Security Functional Requirements of the TOE Objectives

Table 18 below shows a mapping of the objectives and the SFRs that support them.

Table 18 – Objectives:SFRs Mapping

Objective	Requirements Addressing the Objective	Rationale
O.ACCOUN The TOE must provide user	FAU_GEN.1 Audit Data Generation	FAU_GEN.1 meets this objective by providing an audit trail listing all

© 2014 Dell SonicWALL, Inc.
This document may be freely reproduced and distributed whole and intact including this copyright notice.

Objective	Requirements Addressing the Objective	Rationale
accountability for information flows through the TOE and for authorized administrator use of security functions related to audit.		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.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.	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.
	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.AUTHENTICATE 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.	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.
	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.LIMEXT The TOE must provide the means for an authorized administrator to	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

© 2014 Dell SonicWALL, Inc.
This document may be freely reproduced and distributed whole and intact including this copyright notice.

Objective	Requirements Addressing the Objective	Rationale
control and limit access to TOE security functions by an authorized external IT entity.		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.MEDIATE 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 add or delete security attributes in the Information Flow Control List to the Full Administrator in Config Mode role.
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.
	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

© 2014 Dell SonicWALL, Inc.
This document may be freely reproduced and distributed whole and intact including this copyright notice.

Objective	Requirements Addressing the Objective	Rationale
		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 Traffic 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.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.	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

© 2014 Dell SonicWALL, Inc.
This document may be freely reproduced and distributed whole and intact including this copyright notice.

Objective	Requirements Addressing the Objective	Rationale
		for security attributes.
O.SELPRO The TOE must protect itself against attempts by unauthorized users to bypass, deactivate, or tamper with TOE security functions and read, modify, or destroy configuration data.	FIA_UAU.2 User authentication before any action	FIA_UAU.2 meets this objective by ensuring that all administrators must be authenticated prior to accessing TSF functions.
	FIA_UID.2 User identification before any action	FIA_UID.2 meets this objective by requiring that all administrators must be identified prior to accessing TSF functions.
	FMT_MOF.1 Management of security functions behaviour	FMT_MOF.1 meets this objective by ensuring that authenticated administrators are restricted to performing only the actions specified for their role, including certificate management and network configurations.
O.TIME The TOE provides a reliable time stamp.	FPT_STM.1 Reliable time stamps	The TOE provides a reliable time stamp.
O.VPN The TOE must be able to protect the integrity and confidentiality of data transmitted to a peer authorized external IT entity via requests for encryption and authentication for such data. Upon receipt of data from a peer authorized external IT entity, the TOE must be able to request decryption of 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(1) meets this objective by performing cryptographic operations in accordance with specified cryptographic algorithms and key sizes.
	FDP_IFC.1(b) Subset information flow control	FDP_IFC.1(b) meets this objective by defining an information flow control for VPN traffic. This flow control distinguishes VPN traffic from other user data.
	FDP_IFF.1(b) Simple security attributes	FDP_IFF.1(b) meets this objective by defining the rules for the VPN information traffic control policy. This flow control distinguishes VPN traffic from other user data.

© 2014 Dell SonicWALL, Inc.
This document may be freely reproduced and distributed whole and intact including this copyright notice.

Objective	Requirements Addressing the Objective	Rationale
	FDP_ITC.1 Import of user data without security attributes	FDP_ITC.1 meets this objective by allowing the key parameters necessary to establish a VPN to be imported to the TOE.
	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 ensuring that the default VPN Information Flow Control Policy is to use the Traffic Information Flow Control Policy, unless an IPsec header exists.

8.5.2 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 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.2 was chosen to give greater assurance of the developer's on-going flaw remediation process.

8.5.3 Dependency Rationale

The SFRs in this ST satisfy all of the required dependencies listed in the Common Criteria, applicable PPs, and SFRs explicitly stated in this ST. Table 19 lists each requirement to which the TOE claims conformance and indicates whether the dependent requirements are included. As the table indicates, all dependencies have been met.

Table 19 – Functional Requirements Dependencies

SFR ID	Dependencies	Dependency Met	Rationale
FAU_GEN.1	FPT_STM.1	YES	
FAU_SAR.1	FAU_GEN.1	YES	
FAU_SAR.3	FAU_SAR.1	YES	
FCS_CKM.1	FCS_CKM.4	YES	
	FCS_COP.1	YES	
FCS_CKM.4	FCS_CKM.1	YES	
FCS_COP.1	FCS_CKM.4	YES	
	FCS_CKM.1	YES	
FDP_IFC.1(a)	FDP_IFF.1(a)	YES	

© 2014 Dell SonicWALL, Inc.
This document may be freely reproduced and distributed whole and intact including this copyright notice.

SFR ID	Dependencies	Dependency Met	Rationale
FDP_IFC.1(b)	FDP_IFF.1(b)	YES	
FDP_IFF.1(a)	FDP_IFC.1(a)	YES	
	FMT_MSA.3(a)	YES	
FDP_IFF.1(b)	FDP_IFC.1(b)	YES	
	FMT_MSA.3(b)	YES	
FDP_ITC.1	FDP_IFC.1(a)	YES	
	FMT_MSA.3(a)	YES	
FIA_UAU.2	FIA_UID.1	NO	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	n/a	
FMT_MOF.1	FMT_SMR.1	YES	
	FMT_SMF.1	YES	
FMT_MSA.1	FDP_IFC.1(a)	YES	
	FMT_SMF.1	YES	
	FMT_SMR.1	YES	
FMT_MSA.2	FDP_IFC.1(a)	YES	
	FMT_MSA.1	YES	
	FMT_SMR.1	YES	
FMT_MSA.3(a)	FMT_MSA.1	YES	
	FMT_SMR.1	YES	
FMT_MSA.3(b)	FMT_SMR.1	YES	
	FMT_MSA.1	YES	
FMT_SMF.1	No dependencies	n/a	
FMT_SMR.1	FIA_UID.1	NO	Although FIA_UID.1 is not included, FIA_UID.2, which is hierarchical to FIA_UID.1 is included. This satisfies this dependency.
FPT_STM.1	No dependencies	n/a	
FTA_SSL.3	No dependencies	n/a	

© 2014 Dell SonicWALL, Inc.
This document may be freely reproduced and distributed whole and intact including this copyright notice.

9 Acronyms and Terms

This section and Table 20 define the acronyms and terms used throughout this document.

9.1 Acronyms

Table 20 – Acronyms and Terms

Acronym	Definition
3G	Third Generation
3DES	Triple-Data Encryption Standard
AES	Advanced Encryption Standard
ANSI	American National Standards Institute
ARP	Address Resolution Protocol
CA	Certification Authority
CBC	Cipher Block Chaining
CC	Common Criteria
CLI	Command Line Interface
CM	Configuration Management
DHCP	Dynamic Host Configuration Protocol
DMZ	Demilitarized Zone
DNS	Domain Name System
DPI	Deep Packet Inspection
DRBG	Deterministic Random Bit Generator
DSA	Digital Signature Algorithm
EAL	Evaluation Assurance Level
FIPS	Federal Information Processing Standard
GAV	Gateway Anti-Virus
GMS	Global Management System
GUI	Graphical User Interface
HMAC`	Hash Message Authentication Code
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure Sockets Layer(SSL)
ID	Identification
IKE	Internet Key Exchange
IP	Internet Protocol
IPS	Intrusion Prevention System

© 2014 Dell SonicWALL, Inc.
This document may be freely reproduced and distributed whole and intact including this copyright notice.

Acronym	Definition
IPSec	Internet Protocol Security
IT	Information Technology
L2	Layer 2
L2TP	Layer 2 Tunneling Protocol
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
NAT	Network Address Translation
NSA	Network Security Appliance
NTP	Network Time Protocol
OS	Operating System
PP	Protection Profile
PPPoE	Point to Point Protocol over Ethernet
PPTP	Point to Point Tunneling Protocol
RADIUS	Remote Authentication Dial-In User Service
RAM	Random Access Memory
SA	Security Association
SAR	Security Assurance Requirement
SHA	Secure Hash Algorithm
SFP	Security Functional Policy
SFR	Security Functional Requirement
SIP	Session Initiated Protocol
SMTP	Simple Mail Transfer Protocol
SSH	Secure Shell
SSL	Secure Sockets Layer
ST	Security Target
TCBC	Triple DES Cipher Block Chaining
TCP	Transfer Control Protocol
TOE	Target of Evaluation
TSF	TOE Security Functionality
TSP	TOE Security Policy
UDP	User Datagram Protocol
UTM	Unified Threat Management
VoIP	Voice over Internet Protocol

© 2014 Dell SonicWALL, Inc.
This document may be freely reproduced and distributed whole and intact including this copyright notice.

Acronym	Definition
VPN	Virtual Private Network
WAN	Wide Area Network

9.2 Terminology

SPY – Gateway Anti-Spyware

© 2014 Dell SonicWALL, Inc.
This document may be freely reproduced and distributed whole and intact including this copyright notice.

Prepared by:
Corsec Security, Inc.

13135 Lee Jackson Memorial Highway
Suite 220
Fairfax, VA 22033

Phone: +1 703 267 6050
http://www.corsec.com