Citrix Systems, Inc.

NetScaler Platinum Edition Load Balancer Version 9.1

Security Target

Evaluation Assurance Level: EAL2 augmented with ALC_FLR.2

Document Version: 1

Prepared for:

Citrix Systems, Inc.
851 West Cypress Creek Road
Fort Lauderdale, FL 33309

Phone: (954) 267-3000
Email: info@citrix.com
http://www.citrix.com

Prepared by:

Corsec Security, Inc.
10340 Democracy Lane, Suite 201
Fairfax, VA 22030

Phone: (703) 267-6050
Email: info@corsec.com
http://www.corsec.com

Table of Contents

Table of Figures

Table of Tables

References

[CC] Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 3, July 2009

[FIPS] CMVP FIPS 140-2 certificate #870: Nitrox XL NFB FIPS Cryptographic Modules (Hardware Versions: CN1120-VBD-03-0200, CN1010-VBD-03-0200, and CN1005-VBD-03-0200; Firmware Version: 4.6.1)

[AGD Supp] Citrix Systems, Inc. NetScaler Platinum Edition Load Balancer Version 9.1 Guidance Supplement, v1.0

1 Introduction

This section identifies the Security Target (ST), Target of Evaluation (TOE), and the ST organization. The Target of Evaluation is the Citrix NetScaler Platinum Edition Load Balancer Version 9.1, and will hereafter be referred to as the TOE throughout this document. The TOE is the NetScaler 9010-FIPS [FIPS], MPX 7000 Series, MPX 9000 Series, MPX 10000 Series, and MPX 12000 Series hardware appliances and all the installed firmware and software. The NetScaler is a purpose-built application performance accelerator.

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), ST 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 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 (Section 9) – Defines the acronyms and terminology used within this ST.

1.2 Security Target and TOE References

Table 1 – ST and TOE References

ST Title	Citrix Systems, Inc. NetScaler Platinum Edition Load Balancer Version 9.1 Security Target
ST Version	Version 1
ST Author	Corsec Security Inc.
ST Publication Date	3/23/2010
TOE Reference	Citrix NetScaler Platinum Edition Load Balancer Version 9.1 Build 9.1-100.3.cl
Keywords	Citrix, NetScaler, Load Balancer, Proxy, Web Application Firewall, Gateway, Platinum, version 9, LAN, WAN, Performance, Networking, Compression, Optimization, Filtering, Filtration, Scrubbing, Cleansing, VPN

1.3 Product Overview

The NetScaler Platinum Edition Load Balancer Version 9.1 is a dedicated application performance accelerator incorporating a Secure Sockets Layer (SSL) Virtual Private Network (VPN) with policy-based access control and a Web Application Firewall. Figure 1 below shows the details of the deployment configuration of the TOE:

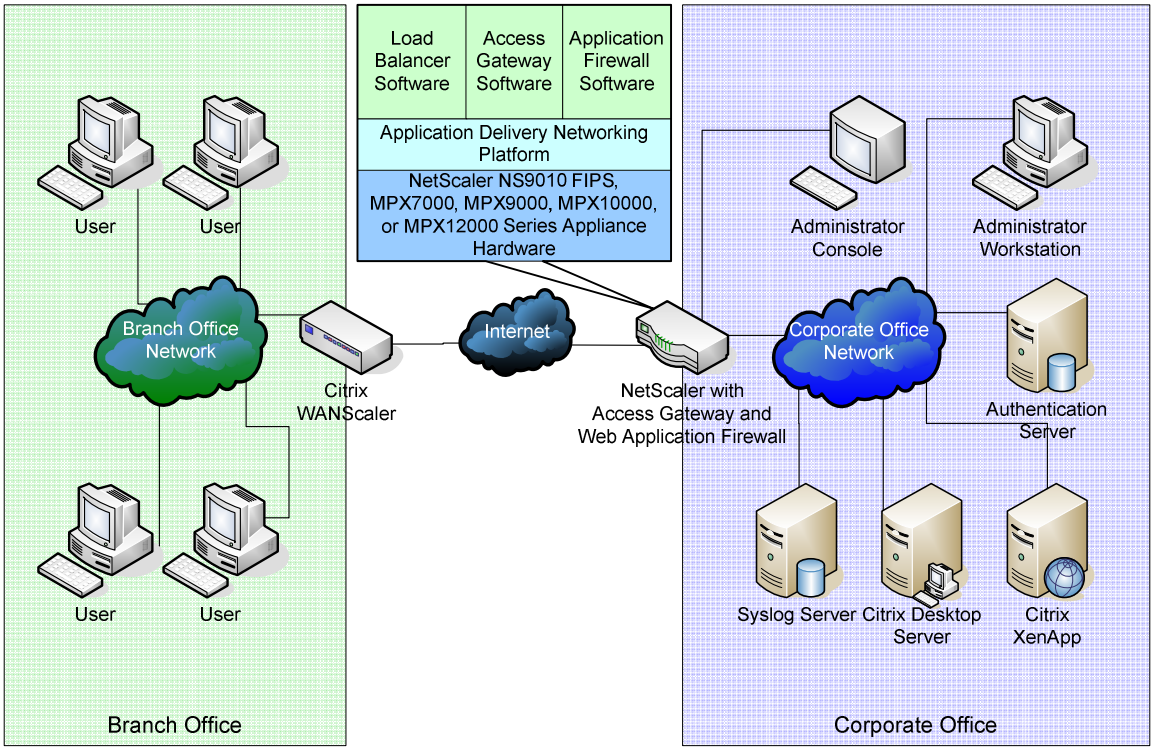

Figure 1 – Deployment Configuration of the Product

The NetScaler appliance incorporates three software components that work together to provide secure access to web-based applications, such as Citrix XenDesktop or XenApp, from an external network. The three software components are the Load Balancer, Access Gateway, and the Web Application Firewall. These run on top of the Application Delivery Networking Platform on the NetScaler 9010-FIPS [FIPS], MPX 7000, MPX 9000, MPX 10000, or MPX 12000 Series Appliance Hardware. These elements are described in the sections below.

TOE Administrators can access the TOE through a direct serial connection. The direct serial connection gives the administrator access to the Command Line Interface (CLI). The CLI can also be accessed from a remote workstation through Secure Shell. TOE administrators can also access the TOE from any workstation on the management network using the NetScaler Configuration Utility. The NetScaler Configuration Utility is accessed via a web browser.

1.3.1 Load Balancer

The Load Balancer component manages the connections between clients and servers. Clients establish a connection with the NetScaler rather than directly with a server. When the NetScaler receives an application request from a client, it establishes a connection with the appropriate application server. This allows the Load Balancer to sort and prioritize application requests from multiple clients and requires only a single connection on the application server to handle requests from multiple clients.

NetScaler can be leveraged to provide optimization by balancing traffic loads across multiple servers. This load balancing is achieved by deploying multiple application servers and allowing NetScaler to balance network traffic among them. Additionally, NetScaler utilizes Transmission Control Protocol (TCP) optimizations and several acceleration technologies to accelerate application performance. The following sections provide descriptions of some of the configurable features provided by the Load Balancer.

1.3.1.1 Load Balancing Virtual Servers

The Load Balancer allows the definition of Load Balancing virtual servers (vserver). Each Load Balancing vserver consists of an IP[1] address, port number, and protocol. A Load Balancing vserver accepts incoming traffic destined for its particular address-port-protocol combination and is mapped to one or more services running on physical servers in a server farm. Clients connect to the Load Balancing virtual server, which directs each request to a physical server. Load Balancing provides methods for each Load Balancing vserver to choose the physical server with the smallest load to direct traffic to.

Each vserver can be configured for a different set of physical services and server and each physical server can offer any number of physical services. The Load Balancer supports protocol- and application-specific vservers for protocols such as HTTP[2], FTP[3], HTTPS[4], NNTP[5], and DNS[6].

1.3.1.2 Content Switching

The Content Switching mechanism of the Load Balancer provides a means for directing HTTP (and HTTPS if configured appropriately) traffic to physical servers based on the content of the traffic. For example, one set of servers may be dedicated to providing dynamic web content, while another set provides static content.

Content Switching is provided by Content Switching vservers. Each Content Switching vserver must be associated with one or more Load Balancing vservers. The Load Balancing vserver then directs the traffic to a physical server based on server load.

1.3.1.3 SSL Acceleration

The Load Balancer component offers SSL Acceleration to relieve web servers of the burden of processing SSL transactions. The Load Balancer intercepts SSL encrypted packets destined for web servers, decrypts them, applies Load Balancing and content switching, and forwards the transactions to the appropriate web server. SSL Acceleration provides a way to ensure the secure delivery of web applications without degrading end-user performance.

---

[1] Internet Protocol
[2] Hypertext Transfer Protocol
[3] File Transfer Protocol
[4] Secure Hypertext Transfer Protocol
[5] Network News Transfer Protocol
[6] Domain Name System

1.3.1.4 AppCache

The Load Balancer utilizes an on-board web cache to speed up content requests. The results of a server request are stored in the cache to be reused to fulfill subsequent requests. This speeds up request time by reducing page regeneration time.

1.3.1.5 AppCompress

The Load Balancer can be configured to use AppCompress, a feature that provides compression between the TOE and the end user. AppCompress uses the DEFLATE compression algorithm[7], which yields up to 50% reduction in bandwidth requirements and improves end-user performance.

1.3.1.6 Surge Protection

Surge Protection within the Load Balancer provides protection against spikes in traffic to managed servers. Surge Protection controls the number of users that can simultaneously access resources on those servers. Additional requests are queued and sent once the server load has lessened. This prevents site overload.

1.3.2 Access Gateway

The Access Gateway component is an SSL VPN which provides policy-based access control for network resources. The Access Gateway allows administrators to control access based on the identity of the user that is connecting and the device that user is connecting from. It can also be configured to have the VPN client run a check on the user's computer to ensure that the latest anti-virus updates are installed before allowing access to mission critical systems.

1.3.3 Web Application Firewall

The Web Application Firewall component provides firewall protection against attacks at the Application Layer of the Open Systems Interconnection Basic Reference Model. It implements a positive security model, which allows only traffic which adheres to industry standards and best coding practices. All other traffic is treated as malicious and blocked.

1.3.4 Application Delivery Networking Platform

The Application Delivery Networking Platform is a highly-specialized kernel and packet processing engine. It coordinates the operations of the other software components and controls the network interfaces, memory management, and system timing. By interfacing closely with the network interface drivers, the Application Delivery Networking Platform is able to guarantee that critical applications receive the highest priority and are not preempted by lower-priority operations.

---

[7] For more information about the DEFLATE compression used, please visit ftp://ftp.uu.net/graphics/png/documents/zlib/zdoc-index.html

1.3.5 Hardware Appliances

The TOE hardware includes the NS 9010-FIPS [FIPS], MPX 7000 Series, MPX 9000 Series, MPX 10000 Series, and MPX 12000 Series hardware appliances. These units support both Fast Ethernet and copper Gigabit Ethernet. All units provide a serial port to connect a computer directly to the unit for management. A Liquid Crystal Display (LCD) on the front of each appliance displays real-time statistics, diagnostics, and alerts. The main difference between the NetScaler units is the number of network ports available, the hardware performance, and the FIPS 140-2 validated crypto card in the 9010-FIPS [FIPS]. See Table 2 for more information.

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 dedicated application performance accelerator incorporating a VPN with policy-based access control. The TOE is located between a Local Area Network (LAN) and a Wide Area Network (WAN), such as a Corporate Office Network and the Internet. Privileged, competent users administer the TOE.

Figure 2 shows the details of the deployment configuration of the TOE:

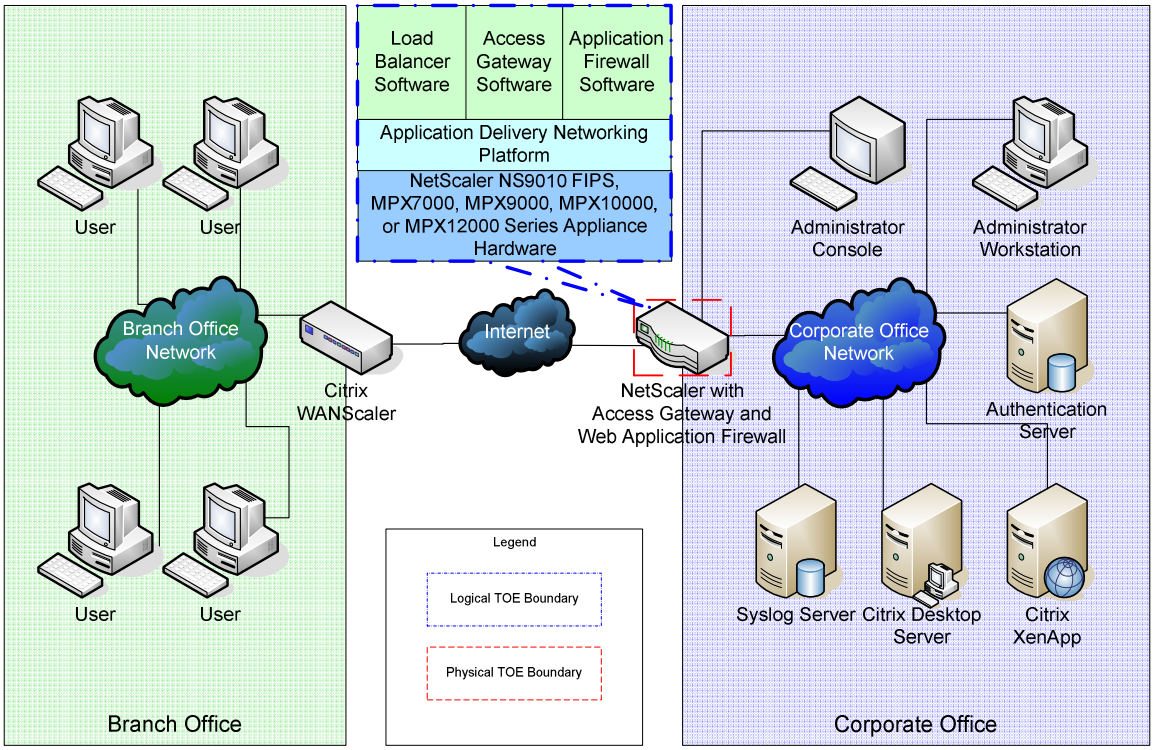

Figure 2 – TOE Boundary

The TOE filters traffic inbound to and outbound from the LAN it is installed on based on a positive security model whereby only traffic that is identified as valid may pass. The TOE provides policy-based access control to LAN resources.

1.4.1 Brief Description of the Components of the TOE

The TOE is composed of the Load Balancer Software, Access Gateway Software, Web Application Firewall Software, and the Application Delivery Networking Platform (NetScaler 9010-FIPS [FIPS], MPX 7000 Series, MPX 9000 Series, MPX 10000 Series, and MPX12000 Series hardware appliances).

1.5 TOE Environment

The TOE environment consists of the following:

- Administrator console and workstation for management
- Application server(s)
- Syslog server (optional)
- VPN client(s)
- Networks (including the Internet and the Corporate Office Network)

- Authentication server (RADIUS[8], LDAP[9])

The TOE is intended to be deployed in a physically secure cabinet, room or data center with the appropriate level of physical access control and physical protection (e.g. fire control, locks, alarms, etc.). The TOE is intended to be managed by administrators operating under a consistent security policy.

The TOE is meant to optimize and protect data traveling from a WAN (including the internet) to a LAN. For the TOE to operate correctly, all optimized and protected traffic must traverse the TOE, and the TOE must be connected to the network in the appropriate deployment configuration. The TOE environment is required to provide for this configuration.

The TOE is managed through a serial CLI and a web-based Graphical User Interface (GUI). Administrators must access these interfaces from a trusted workstation that supports SSH and a web browser. The CLI and web GUI are part of the TOE. The administrator accesses the CLI through an SSH client or serial connection and the web GUI through a standard web browser.

1.6 TOE Description

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

1.6.1 Physical Scope

Figure 2 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 an application performance accelerator[10] running on a NetScaler 9010-FIPS [FIPS], MPX 7000 Series, MPX 9000 Series, MPX 10000 Series, and MPX12000 Series hardware appliance. The TOE is installed between a LAN and a WAN as depicted in Figure 2.

1.6.1.1 TOE Appliance Hardware

The TOE software runs on a NetScaler 9010-FIPS [FIPS], MPX 7000 Series, MPX 9000 Series, MPX 10000 Series, and MPX 12000 Series hardware appliance. Table 2 specifies the hardware specifications for the proper operation of the TOE.

Table 2 – TOE Hardware Specifications

Category	Requirement

[8] Remote Authentication Dial In User Service
[9] Lightweight Directory Access Protocol

[10] The developer refers to the TOE as a Load Balancer, so the title of the ST and of the TOE includes this terminology.

Category	Requirement
9010-FIPS [FIPS]	• Single Processor, 2U unit. • 2 gigabytes (GB) of memory. • System throughput of 2 gigabits per second (Gbps).
MPX 7000 and 9000 Series	• Multi-core processor, 1U unit • 8GB of memory. • System throughput ranging from 1-3 Gbps.
MPX 10000 and 12000 Series	• Multi core processor, 2U unit. • 16GB of memory. • System throughput ranging from 5-8 Gbps.

1.6.1.2 Guidance Documentation

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

- Citrix NetScaler Hardware Installation and Setup Guide Citrix© NetScaler© 9.1
- Citrix NetScaler Command Reference Guide Citrix© NetScaler© 9.1
- Citrix NetScaler v9.1 Guidance Supplement [AGD Supp]

1.6.2 Logical Scope

The logical boundary is shown in Figure 2 above. There are several logical components of the TOE: the 9010-FIPS [FIPS], MPX 7000 Series, MPX 9000 Series, MPX 10000 Series, or MPX12000 Series Application Delivery Networking Platform, the Load Balancer Software, the Access Gateway Software, and the Web Application Firewall Software. These components work together to provide the TOE Security Functions (TSFs).

The TOE's logical boundary includes all of the TSFs. The SFRs implemented by the TOE are usefully grouped under the following Security Function Classes:

- FAU Security Audit
- FDP User Data Protection
- FIA Identification and Authentication
- FMT Security Management
- FPT Protection of the TSF

These functions are discussed in detail below.

1.6.2.1 Security Audit

The Security Audit function provides the generation, storing, and review of audit records. Audit data is generated by the TOE and stored locally. The TOE controls access to the audit data and protects it from unauthorized deletion or modification. The audit data is presented to TOE users in a manner suitable for human readability and portions of the audit records are searchable.

1.6.2.2 User Data Protection

The TOE enforces three Security Functional Policies (SFPs): the Administrator Access Control SFP, the VPN Access Control SFP, and the VPN Information Flow Control SFP. These SFPs are enforced on subjects, objects and operations. The TOE ensures that operations between subjects on objects that fall under these SFPs are regulated by the TOE based on the criteria defined by the SFPs.

1.6.2.3 Identification and Authentication

Identification and authentication is performed against user information stored locally on the TOE or user information stored on an external RADIUS or LDAP Server. The TOE ensures that users and administrators are identified and authenticated prior to any use of the TOE functions. The TOE supports authentication via username and password combinations.

1.6.2.4 Security Management

The TOE maintains four vendor-defined roles: read-only, operator, network, and superuser. It also allows custom roles to be defined by administrators. These roles (which are commonly referred to as "administrators" throughout this document) have different levels of access to TSF data, security functions, and security attributes. After successful authentication to the TOE, administrators can access only the management functions to which their roles grant them access.

1.6.2.5 Protection of the TSF

The TOE provides a reliable time stamp mechanism for its own use.

1.6.3 Product Physical/Logical Features and Functionality not included in the TOE

The TOE includes the following features:

- Load Balancing Virtual Servers
- SSL VPN
- Application Firewall

The following features are excluded from the TOE:

- Content Switching
- Content Rewrite

- Caching
- Compression
- Web Logging
- Layer 3 Routing
- Load Balancing between NetScaler appliances

In addition, any other features or functionality not mentioned explicitly in Sections 1.4 and 1.6 are excluded from the TOE.

2 Conformance Claims

This section provides 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 3, September 2007[CC]; CC Part 2 conformant; CC Part 3 conformant; PP claim (none); Parts 2 and 3 Interpretations of the CEM as of 2009/07 were reviewed, and no interpretations apply to the claims made in this ST.
PP Identification	None
Evaluation Assurance Level	EAL2 augmented with ALC_FLR.2

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 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 a 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 basic level of motivation. The IT assets requiring protection are the user data and system 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. The following threats are applicable:

Table 4 – Threats

Name	Description
T.ACCESSINT	A user may gain unauthorized access to internal network resources.
T.ACCESSTOE	A user may gain unauthorized access to security data on the TOE.
T.AVAIL	An authorized user may not be able to utilize NetScaler services due to physical tampering of the TOE or the network.

Name	Description
T.MASQUERADE	A user or process may masquerade as another entity in order to gain unauthorized access to data or TOE resources.
T.MODCONF	An attacker or unauthorized user may modify a user's configuration. This covers: modification of the user's set of permitted internal network resources modification of configuration data associated with a user.
T.TAMPERING	A user or process may be able to bypass the TOE's security mechanisms thereby compromising TOE user or system data.

3.2 Organizational Security Policies

No organizational security policies apply to the TOE.

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. The following specific conditions are required to ensure the security of the TOE and are assumed to exist in an environment where this TOE is employed.

Table 5 – Assumptions

Name	Description
A.CRYPTO	The TOE environment will ensure that the TOE stored cryptographic data is protected against tampering.
A.DISCLOSE	Users and administrators will not disclose their passwords.
A.EXTERNAL	The external authentication servers are operating correctly and securely. Data transmitted between the TOE and the external servers is protected from tampering by un-trusted subjects during transfer to the external server, during storage on the external server, and during transmission to the TOE from the external server.

Name	Description
A.INSTALL	The TOE has been installed and configured according to the appropriate installation guides, and all traffic between the internal and external networks flows through it.
A.LOCATE	The TOE is located within a controlled access facility which restricts physical access to the appliance to authorized persons only, and provides uninterruptible power, air conditioning, and all other conditions required for reliable operation of the hardware.
A.MANAGE	There is one or more competent individual (administrator) assigned to manage the TOE and the security of the information it contains.
A.NETCON	The TOE environment provides the required network connectivity and the connectivity is protected from tampering. TOE Management will only be performed from the internal protected network.
A.NOEVIL	The users who manage the TOE are non-hostile, appropriately trained, and follow all guidance.
A.PASSWORDS	Administrators and users will set passwords of at least eight characters that are not dictionary words or combinations of dictionary words, using a combination of uppercase, lowercase, numeric, and symbolic characters.

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 as follows:

Table 6 – Security Objectives for the TOE

Name	Description
O.ADMIN	The TOE must include a set of functions that allow management of its functions and data, ensuring that TOE users with the appropriate privileges and only those TOE users, may exercise such control.
O.AUDIT	The TOE must record the actions taken by administrators (except actions performed at the underlying FreeBSD shell), prevent unauthorized deletion of the audit records stored on the TOE, and provide the authorized administrators with the ability to review the audit trail.
O.AUTHENTICATE	The TOE must be able to identify and authenticate administrators prior to allowing access to TOE administrative functions and data.
O.INTACC	The TOE must allow access to internal network resources only as defined by the VPN User Access Control SFP and the VPN User Information Flow Control SFP.
O.EXTACC	The TOE must allow access to external IT entities sending or receiving traffic through the TOE only as defined by the Web Application Firewall Information Flow Control SFP.
O.TIME	The TOE must provide reliable timestamps for its own use.

4.2 Security Objectives for the Operational Environment

The following section describes the security objectives that must be met by the TOE operational environment.

4.2.1 IT Security Objectives

The following IT security objectives are to be satisfied by the environment:

Table 7 – IT Security Objectives

Name	Description
OE.CONNECT	The TOE environment must provide network connectivity to the TOE. The network connection to the TOE must be reliable.
OE.EXTERNAL	The TOE environment must ensure any authentication data in the environment are protected and maintained.
OE.CRYPTO	The TOE environment must ensure that the stored cryptographic data is protected against tampering.

4.2.2 Non-IT Security Objectives

The following non-IT environment security objectives 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.AC	The TOE environment must regulate the temperature of the facility where the TOE is located so no damage is caused by heat or cold.

Name	Description
NOE.CREDENTIALS	Users and administrators will set secure passwords and will protect their access credentials.
NOE.INSTALL	Those responsible for the TOE must ensure that the TOE is delivered, installed, managed, and operated in a manner which is consistent with common IT security policies. The TOE must be installed such that all traffic between the internal and external networks flows through it.
NOE.MANAGE	Sites deploying the TOE will provide competent, non-hostile TOE administrators who are appropriately trained and follow all administrator guidance. TOE administrators will ensure the system is used securely. The reliability of the TOE's timestamps will be ensured via periodic manual checks by the TOE administrator.
NOE.PHYSICAL	The physical environment must be suitable for supporting a computing device in a secure setting.
NOE.POWER	The TOE environment must provide the electricity necessary to the TOE to function. The power to the TOE must be reliable and protected from surges and disconnects.

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

No extended TSF components apply to the TOE.

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 italicized 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	✓	✓		
FAU_STG.1	Protected audit trail storage	✓			

Name	Description	S	A	R	I
FDP_ACC.1(a)	Subset access control		✓		✓
FDP_ACC.1(b)	Subset access control		✓		✓
FDP_ACF.1(a)	Security attribute based access control		✓		✓
FDP_ACF.1(b)	Security attribute based access control		✓		✓
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		✓		
FIA_UAU.2	User authentication before any action				
FIA_UID.2	User identification before any action				
FMT_MOF.1	Management of security functions behaviour	✓	✓		
FMT_MSA.1	Management of security attributes	✓	✓	✓	
FMT_MSA.3(a)	Static attribute initialisation	✓	✓		✓
FMT_MSA.3(b)	Static attribute initialisation	✓	✓		✓
FMT_MSA.3(c)	Static attribute initialisation	✓	✓		✓
FMT_MSA.3(d)	Static attribute initialisation	✓	✓		✓
FMT_MTD.1	Management of TSF data	✓	✓	✓	
FMT_SMF.1	Specification of management functions		✓		

Name	Description	S	A	R	I
FMT_SMR.1	Security roles		✓		
FPT_STM.1	Reliable timestamps			✓	

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

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:

- Start-up and shutdown of the audit functions;
- All auditable events, for the [*not specified*[11]] level of audit; and
- [*All administrator-executed commands (including failed login attempts).*]

FAU_GEN.1.2

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

- Date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event; and
- For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [*the IP address of the user.*]

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 [*network, super user, and additional custom defined roles as defined by an administrator*] 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.

---

[11] There is only one level of audit.

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*] of audit data based on [*keywords through the CLI and GUI.*]

Dependencies: FAU_SAR.1 Audit review

FAU_STG.1 Protected audit trail storage

Hierarchical to: No other components.

FAU_STG.1.1

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

FAU_STG.1.2

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

Dependencies: FAU_GEN.1 Audit data generation

Application Note: Since the TOE audit logs might contain sensitive data critical to the security of the TOE, the TOE administrator must ensure that only authorized administrators have access to the audit logs on the TOE and any backups of the audit logs that might exist outside of the TOE. If a backup of the audit logs is created (for example, to an external syslog server), the administrator must ensure that the audit logs are protected from disclosure to non-TOE administrators during transmission and storage.

6.2.2 Class FDP: User Data Protection

FDP_ACC.1(a) Subset access control – Administrator Access Control

Hierarchical to: No other components.

FDP_ACC.1.1(a)

The TSF shall enforce the [*Administrator Access Control SFP*] on [*the following:*

Subjects:

- *Administrators*

Objects:

- *Commands*

Operations:

- *Execute*]

Dependencies: FDP_ACF.1 Security attribute based access control

FDP_ACC.1(b) Subset access control – VPN Access Control

Hierarchical to: No other components.

FDP_ACC.1.1(b)

The TSF shall enforce the [*VPN Access Control SFP*] on [*the following:*

[*Subjects:*

- *VPN Clients*

Objects:

- *VPN connections*

Operations:

- *Establish*
- *Disconnect*]

Dependencies: FDP_ACF.1 Security attribute based access control

FDP_ACF.1(a) Security attribute based access control – Administrator Access Control

Hierarchical to: No other components.

FDP_ACF.1.1(a)

The TSF shall enforce the [*Administrator Access Control SFP*] to objects based on the following:

[*Subjects:*

- *Administrators*

Subject Attributes:

- *Roles assigned to administrators or assigned to an administrator's group*

Objects:

- *Commands*

Object Attributes:

- *None*]

FDP_ACF.1.2(a)

The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed:

- [*The administrator is granted execute permission for a command if the administrator is assigned a role or is a member of a group which is assigned a role that:*

  a. contains an allow policy for the command and

  b. the role is a higher priority than any other applicable role containing a deny policy for that command.

- *The administrator is not granted execute permission for a command if the administrator is assigned a role or a member of a group which is assigned a role that:*

  a. contains a deny policy for the command and

  b. the role is a higher priority than any other applicable role containing an allow policy for that command.

- *The administrator is not granted execute permission for a command if the administrator is not:*

    a. *assigned a role that contains an allow or deny policy for the command and*

    b. *is not a member of a group which is assigned a role that contains an allow or deny policy for the command.*

- *If two (or more) applicable policies have the same priority, then the policy which is loaded first in the set of policies is applied to the command.*]

FDP_ACF.1.3(a)

The TSF shall explicitly authorise access of subjects to objects based on the following additional rules:

[*All administrators are given execute permission to the following commands:*

- *show cli attribute*
- *clear cli prompt*
- *alias*
- *unalias*
- *help*
- *history*
- *quit*
- *exit*
- *whoami*
- *config*
- *set cli mode*
- *show cli mode*
- *set cli prompt*
- *show cli prompt*

]

FDP_ACF.1.4(a)

The TSF shall explicitly deny access of subjects to objects based on the following additional rules*:*

[*Any administrator that is not assigned a role and not a member of any group that has been assigned a role will be denied access to all commands other than those listed in FDP_ACF.1.3(a).*]

Dependencies: **FDP_ACC.1(a) Subset access control**
FMT_MSA.3(a) Static attribute initialization

FDP_ACF.1(b) Security attribute based access control – VPN Access Control

Hierarchical to: No other components.

FDP_ACF.1.1(b)

The TSF shall enforce the [*VPN Access Control SFP*] to objects based on the following:

[*Subjects:*

- *VPN Clients*

Subject Attributes:

- *Username*
- *Password*
- *SSL Certificate attributes*
- *Source IP*[12] *address and/or subnet mask*

Objects:

- *VPN Connections*

Object Attributes:

- *Day and time accessible*]

FDP_ACF.1.2(b)

The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed:

[*If the user supplies the correct credentials, is found in the configured database, and is logging in at an acceptable day and time, the user is granted establish rights.*

Else, the user is denied establish rights.

A user is given disconnect to a VPN connection only if he is the owner of the VPN connection.]

[12] Internet Protocol

FDP_ACF.1.3(b)

The TSF shall explicitly authorise access of subjects to objects based on the following additional rules:

- [*No additional rules.*]

FDP_ACF.1.4(b)

The TSF shall explicitly deny access of subjects to objects based on the following additional rules:

- [*No additional rules.*]

Dependencies: **FDP_ACC.1(b) Subset access control**
FMT_MSA.3(b) Static attribute initialization

FDP_IFC.1(a) Subset information flow control

Hierarchical to: No other components.

FDP_IFC.1.1(a)

The TSF shall enforce the [*VPN Information Flow Control SFP*] on [*the following:*

[*Subjects:*

- *VPN Clients*

Information:

- *Internal Network Resources*

Operation:

- *Access*]

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 [*Web Application Firewall Information Flow Control SFP*] on [*the following:*

Subjects:

- *Internal or external IT entities sending or receiving traffic through the TOE,*

Information:

- *network traffic flowing through the TOE, and*

Operation:

- *Access*]

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

[*Subjects:*

- *VPN Clients*

Subject Attributes:

- *Username*
- *Group*

Information:

- *Internal Network Resources*

Information Attributes:

Server IP address and port number

Intranet domain]

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:

- [*The user has been granted access to the resource by an administrator or*
- *The user is a member of a group that has been granted access to the resource by an administrator*.]

FDP_IFF.1.3(a)

The TSF shall enforce the

[*no additional information flow control SFP rules*.]

FDP_IFF.1.4(a)

The TSF shall explicitly authorise an information flow based on the following rules:

[*no additional rules*.]

FDP_IFF.1.5(a)

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

[*no additional rules*.]

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

FDP_IFF.1(b) Simple security attributes

Hierarchical to: No other components.

FDP_IFF.1.1(b)

The TSF shall enforce the [*Web Application Firewall Information Flow Control SFP*] based on the following subject security attributes and information security attributes:

[*Subjects:*

- *Internal or external IT entities*

Subject Attributes:

- *Source Uniform Resource Locator (URL)*

- *Source IP address*

Information:

- *Network traffic*
- *IT resource (identified by destination IP address)*

Information Attributes:

- *Destination IP address*
- *HTTP method used in the connection request*
- *URL tokens in the HTTP header*
- *HTTP version of the connection*
- *HTTP header contents (including source and destination IP addresses)*
- *Length of the contents of the URL header*
- *URL header query*
- *Length of the URL header query*]

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: [

1. *The internal or external IT entity has been granted access to the resource by an administrator based on the subject attributes and*
2. *the network traffic information originating from the internal or external IT entity has been granted access by an administrator based on the information attributes*].

FDP_IFF.1.3(b)

The TSF shall enforce the

- [*default condition of denying traffic that has not been authorized by an administrator.*]

FDP_IFF.1.4(b)

The TSF shall explicitly authorise an information flow based on the following rules:

- [*No additional rules.*]

FDP_IFF.1.5(b)

The TSF shall explicitly deny an information flow between a controlled subject and controlled information via a controlled operation based on the following rules: [

1. *The internal or external IT entity has been denied access to the resource by an administrator based on the subject attributes or*

2. *the network traffic information originating from the internal or external IT entity has been denied by an administrator based on the information attributes*].

Dependencies: **FDP_IFC.1(b) Subset information flow control**
FMT_MSA.3(d) Static attribute initialization

6.2.3 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 to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

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 to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

Dependencies: No dependencies

6.2.4 Class FMT: Security Management

The table below represents the access control matrix for the NetScaler administrator roles. It is referenced in the definition of FMT_MOF.1, FMT_MSA.1, and FMT_MTD.1.

Table 10 – FMT Access Control Matrix

Role / Security Attributes	read-only	operator	network	superuser	custom defined role
Administrator roles				Create, delete, query, modify	As defined
Administrator groups				Create, delete, query, modify	As defined
Role policies				Create, delete, query, modify	As defined
Role priorities				Create, delete, query, modify	As defined
VPN user groups	Query	Query, modify	Create, delete, query, modify	Create, delete, query, modify	As defined
VPN user permissions	Query	Query, modify	Create, delete, query, modify	Create, delete, query, modify	As defined
Web Application Firewall permissions	Query	Query, modify	Create, delete, query, modify	Create, delete, query, modify	As defined
Functions					
SSL VPN	Determine the behaviour of	Determine the behaviour of	Determine the behaviour of, modify the behaviour of	Determine the behaviour of, modify the behaviour of	As defined
Web Application Firewall	Query the behaviour of	Modify the behaviour of	Determine the behaviour of, modify the behaviour of	Determine the behaviour of, modify the behaviour of	As defined
Audit	Determine the behaviour of	Determine the behaviour of	Determine the behaviour of	Determine the behaviour of, modify the behaviour of	As defined

Role Security Attributes	read-only	operator	network	superuser	custom defined role
TSF Data					
Audit data				Query, delete	As defined
Administrator accounts				Create, delete, query, modify	As defined
VPN user accounts	Query	Create, delete, query, modify	Create, delete, query, modify	Create, delete, query, modify	As defined
Web Application Firewall Subject Attributes			Create, delete, query, modify	Create, delete, query, modify	As defined

Note regarding Access Control Matrix: "nsroot" (default administrator account) and "superuser" are the only accounts allowed to access the Audit data via Secure Shell File Transfer Protocol (SFTP) or Secure Copy (SCP) protocols – all other accounts will be denied access. The nsroot account provides complete access to all features of the NetScaler.

FMT_MOF.1 Management of security functions behaviour

Hierarchical to: No other components.

FMT_MOF.1.1

The TSF shall restrict the ability to [*determine the behaviour of or modify the behaviour of*] the functions [*listed in Table 10 above*] to [*the administrator roles listed in Table 10 above*].

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 [*Administrative Access Control SFP*] to restrict the ability to [*query, modify, delete, or create* **as specified in Table 10 above**] the security attributes [*listed in Table 10 above*] to [*the administrative roles outlined in Table 10 above*].

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

FMT_MSA.3(a) Static attribute initialisation

Hierarchical to: No other components.

FMT_MSA.3.1(a)

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

FMT_MSA.3.2(a)

The TSF shall allow the [*superuser and authorised custom defined roles*] to specify alternative initial values to override the default values when an object or information is created.

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

FMT_MSA.3(b) Static attribute initialisation

Hierarchical to: No other components.

FMT_MSA.3.1(b)

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

FMT_MSA.3.2(b)

The TSF shall allow the [*network, superuser and authorised custom defined roles*] 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(c) Static attribute initialisation

Hierarchical to: No other components.

FMT_MSA3.1(c)

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(c)

The TSF shall allow the [*superuser and authorised custom defined roles*] 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(d) Static attribute initialisation

Hierarchical to: No other components.

FMT_MSA.3.1(d)

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

FMT_MSA.3.2(d)

The TSF shall allow the [*network, superuser and authorised custom defined roles*] 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_MTD.1 Management of TSF data

Hierarchical to: No other components.

FMT_MTD.1.1

The TSF shall restrict the ability to [*query, modify, delete, or create* **as specified in Table 10 above**] the [*TSF data listed in Table 10 above*] to [*the administrative roles listed in Table 10 above*].

Dependencies: **FMT_SMF.1 Specification of management functions**

FMT_SMR.1 Security roles

FMT_SMF.1 Specification of Management Functions

Hierarchical to: No other components.

FMT_SMF.1.1

The TSF shall be capable of performing the following **security** management functions:

- [*Query and modify administrator roles, administrator accounts, administrator groups, administrator role policies, and administrator role priorities.*
- *Query and modify VPN user accounts, VPN user groups, and VPN user permissions.*
- *Query and delete audit records.*
- *Modify (enable and disable) SSL VPN functionality.*
- *Modify (enable and disable) Web Application Firewall functionality.*]

Dependencies: No Dependencies

FMT_SMR.1 Security roles

Hierarchical to: No other components.

FMT_SMR.1.1

The TSF shall maintain the roles [*read-only, operator, network, superuser, and custom defined roles defined by an administrator*].

FMT_SMR.1.2

The TSF shall be able to associate users with roles.

Dependencies: FIA_UID.1 Timing of identification

6.2.5 Class FPT: Protection of the TSF

FPT_STM.1 Reliable time stamps

Hierarchical to: No other components.

FPT_STM.1.1

The TSF shall be able to provide reliable time stamps **for its own use**.

Dependencies: No dependencies

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 EAL2 augmented with ALC_FLR.2. Table 11 – Assurance Requirements summarizes the requirements.

Table 11 – Assurance Requirements

Assurance Requirements	
Class ASE: Security Target Evaluation	ASE_CLL.1 Conformance Claims
	ASE_ECD.1 Extended components definition
	ASE_INT.1 ST introduction
	ASE_OBJ.2 Security objectives
	ASE_REQ.2 Delivered security requirements
	ASE_SPD.1 Security problem definition
	ASE_TSS.1 TOE Summary specification
Class ALC : Life Cycle Support	ALC_CMC.2 Use of a CM system
	ALC_CMS.2 Parts of the TOE CM coverage
	ALC_DEL.1 Delivery Procedures
	ALC_FLR.2 Flaw reporting procedures
Class ADV: Development	ADV_ARC.1 Security Architecture Description
	ADV_FSP.2 Security-enforcing functional specification
	ADV_TDS.1 Basic design
Class AGD: Guidance documents	AGD_OPE.1 Operational user guidance
	AGD_PRE.1 Preparative procedures
Class ATE: Tests	ATE_COV.1 Evidence of coverage
	ATE_FUN.1 Functional testing
	ATE_IND.2 Independent testing – sample
Class AVA: Vulnerability assessment	AVA_VAN.2 Vulnerability analysis

7 TOE 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 12 – Mapping of TOE Security Functions to Security Functional Requirements

TOE Security Function	SFR ID	Description
Security Audit	FAU_GEN.1	Audit data generation
	FAU_SAR.1	Audit review
	FAU_SAR.3	Selectable audit review
	FAU_STG.1	Protected audit trail storage
User Data Protection	FDP_ACC.1(a)	Subset access control
	FDP_ACC.1(b)	Subset access control
	FDP_ACF.1(a)	Security attribute based access control
	FDP_ACF.1(b)	Security attribute based access control
	FDP_IFC.1(a)	Subset information flow control
	FDP_IFC.1(b)	Subset information flow control
	FDP_IFF.1(a)	Simple security attributes

TOE Security Function	SFR ID	Description
	FDP_IFF.1(b)	Simple 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.3(a)	Static attribute initialisation
	FMT_MSA.3(b)	Static attribute initialisation
	FMT_MSA.3(c)	Static attribute initialisation
	FMT_MSA.3(d)	Static attribute initialisation
	FMT_MTD.1	Management of TSF data
	FMT_SMF.1	Specification of management functions
	FMT_SMR.1	Security roles
Protection of the TSF	FPT_STM.1	Reliable timestamps

7.1.1 Security Audit

Administrators access the TOE either through the CLI or the NetScaler Configuration Utility. The TOE generates audit records for commands executed on either of these interfaces. The audit contents consist of the identification of the administrator who performed the operation, the IP address of the machine if connecting remotely, the date and time of the event, the exact command (with selected options) that the

administrator attempted to execute, and an indication of the success or failure of the command. (FAU_GEN.1)

The audit records are stored on the TOE in "/var/logs." The TOE protects the audit records so that only the authorized administrators (those with the nsroot, superuser, or a custom allowed role) can read or delete them. (FAU_STG.1)

The TOE provides the capability to read the audit records through the CLI and through the NetScaler Configuration Utility. Searches of the audit records based on keywords can also be performed through the CLI by utilizing the grep command. Searches of the audit records can also be performed through the GUI Configuration Applet. The GUI Configuration Applet allows administrators to filter messages based on the module, event type and severity. In addition, there is a Search string facility for the message allowing it to be searched on any field contained in the message including: Command, Remote_ip, Status, and User. (FAU_SAR.1, FAU_SAR.3, FMT_MTD.1, FMT_SMF.1)

TOE Security Functional Requirements Satisfied: FAU_GEN.1, FAU_SAR.1, FAU_SAR.1, FAU_SAR.3, FAU_STG.1, FMT_MTD.1, and FMT_SMF.1

7.1.2 User Data Protection

The TOE enforces the following SFPs:

7.1.2.1 Administrator Access Control SFP

The Administrator Access Control SFP is applied to administrators when they access the NetScaler through the CLI or the NetScaler Configuration Utility. (FDP_ACC.1(a))

Administrators are assigned roles or are members of groups that have roles assigned to them. An administrator or group may have more than one assigned role and an administrator may belong to more than one group. There are four roles predefined by the NetScaler: *superuser*, *network*, *operator*, and *read-only*. Administrators in the superuser role can also define custom roles and assign these roles to administrators and groups. The administrator's role determines which commands the administrator can execute. Roles are assigned priorities on per user and per group basis. Priority is given first to roles assigned directly to the administrator then to roles assigned to the administrator's groups. (FDP_ACF.1(a))

The following rules apply:

- The administrator is granted *execute* permission for a command if the administrator is assigned a role or is a member of a group which is assigned a role that: (a) contains an *allow* policy for the command and (b) is a higher priority than any other applicable role containing a *deny* policy for that command.

- The administrator is not granted *execute* permission for a command if the administrator is assigned a role or a member of a group which is assigned a role that: (a) contains a *deny*

policy for the command and (b) is a higher priority than any other applicable role containing an *allow* policy for that command.

- The administrator is not granted *execute* permission for a command if the administrator is (a) not assigned a role that contains an *allow* or *deny* policy for the command and (b) not a member of a group which is assigned a role that contains an *allow* or *deny* policy for the command.
- All administrators are given *execute* permission to the command "help."
- Any administrator that is not assigned a role and not a member of any group that has been assigned a role will be denied access to all other commands.
- If two (or more) applicable policies have the same priority, then the policy which is loaded first in the set of policies is applied to the command. (FDP_ACF.1(a))

7.1.2.2 VPN Access Control SFP

If configured, the SSL VPN Access Control SFP controls VPN users establishing VPN connections to the NetScaler. (FDP_ACC.1b)

Users can be authenticated based on their username, password, client SSL certificate attributes, source IP and netmask, and the day and time the user is logging in. If a user supplies the correct credentials, the user is allowed to establish a VPN connection. Otherwise, the user is denied. Authentication data for users is either stored locally or in a remote authentication server. (FDP_ACF.1(b), FIA_UAU.2, FIA_UID.2)

The user may terminate the connection by logging out or closing the VPN window. A user can disconnect only his VPN connection. (FDP_ACF.1(b))

7.1.2.3 VPN Information Flow Control SFP

Once a user is authenticated and granted a VPN connection by the SSL VPN Access Control SFP, the SSL VPN Information Flow Control SFP controls access by the user to network resources. Network resources include: intranet and extranet websites, shared Windows file systems, and internal client/server applications. (FDP_IFC.1(a))

The administrator configures which resources are accessible to each user. If the user has been granted access permission to a resource, they are allowed to access it. Otherwise the user is denied. (FDP_IFF.1(a))

7.1.2.4 Web Application Firewall Information Flow Control SFP

The TOE only allows HTTP traffic that meets specific criteria to traverse itself. Any external IT device that sends or receives traffic through the TOE must be able to meet the TOE Web Application Firewall's communication criteria. (FDP_IFC.1(b))

The external IT device is able to send and receive information through the TOE if it has been administratively allowed to do so by being enabled in TOE Web Application Firewall settings. Traffic must possess the administratively-configured security and information attributes to pass through the TOE Web Application Firewall. If the external IT device traffic has been granted access permission to the TOE Web Application Firewall, they may pass traffic through it. Otherwise the external IT device is denied. (FDP_IFF.1(b))

External IT devices are by default not allowed to send traffic through the TOE Web Application Firewall. Administrators must authorise an external IT device to send traffic through the TOE Web Application Firewall. These lists of authorizations comprise the Web Application Firewall rules. (FDP_IFF.1(b))

TOE Security Functional Requirements Satisfied: FDP_ACC.1(a), FDP_ACC.1(b), FDP_ACF.1(a), FDP_ACF.1(b), FDP_IFC.1(a), FDP_IFC.1(b), FDP_IFF.1(a), FDP_IFF.1(b), FIA_UAU.2, and FIA_UID.2.

7.1.3 Identification and Authentication

Administrators access the TOE either through the CLI or the NetScaler Configuration Utility. Identification and authentication is required for administrators accessing the TOE through either interface before access is given to any of the TOE functions. Users access the TOE through the SSL VPN. Users must also be identified and authenticated before being given access to VPN tunnels on the TOE. IDs and passwords can be stored locally or on an external RADIUS or LDAP Server. (FIA_UAU.2, FIA_UID.2)

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

7.1.4 Security Management

The TOE maintains four developer-defined administrator roles and allows additional roles to be defined by authorized administrators through role policies. (FMT_SMR.1)

The TOE provides these administrators the ability to perform management functions based on their assigned roles. Access privileges to TSF data, user attributes, and security functions for the different roles are defined in Table 10 above. (FMT_MOF.1, FMT_MSA.1, FMT_MTD.1)

The management functions provided by the TOE are:

- Query and modify administrator roles, administrator accounts, administrator groups, administrator role policies, and administrator role priorities.
- Query and modify VPN user accounts, VPN user groups, and VPN user permissions.
- Query and delete audit records.
- Modify (enable and disable) SSL VPN functionality
- Modify (enable and disable) Web Application Firewall functionality. (FMT_SMF.1)

The TOE also manages the SFPs discussed in Section 7.1.2 by providing restrictive default values for the security attributes that are used to enforce the SFPs. Specific roles can override the default values and specify alternative initial values. (FMT_MSA.3(a), FMT_MSA.3(b), FMT_MSA.3(c), FMT_MSA.3(d))

TOE Security Functional Requirements Satisfied: FMT_MOF.1, FMT_MSA.1, FMT_MSA.3(a), FMT_MSA.3(b), FMT_MSA.3(c), FMT_MTD.3(d), FMT_MTD.1, FMT_SMF.1, and FMT_SMR.1.

7.1.5 Protection of the TSF

The TOE hardware provides timestamps for the TOE's use. The timestamps are used to support the Security Audit TSF and the User Data Protection TSF. (FPT_STM.1)

TOE Security Functional Requirements Satisfied: FPT_STM.1.

8 Rationale

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

8.1 Conformance Claims Rationale

This Security Target conforms to Part 2 and Part 3 of the Common Criteria Standard for Information Technology Security Evaluations, version 3.1, revision 3.

8.2 Extended Security Functional Requirements

No extended SFRs have been claimed in this Security Target.

8.3 Protection Profile Claims Rationale

There are no protection profile claims for this Security Target.

8.4 Security Objectives Rationale

This section provides a rationale for the existence of each threat, policy statement, and assumption that compose the Security Target. Sections 8.4.1, 8.4.2, and 8.4.3 demonstrate the mappings between the threats, polices, and assumptions to the security objectives is complete. The following discussion provides detailed evidence of coverage for each threat, policy, and assumption.

8.4.1 Security Objectives Rationale Relating to Threats

Table 13 maps threats to objectives.

Table 13 – Threats:Objectives Mapping

Threats	Objectives	Rationale
T.ACCESSINT A user may gain unauthorized	NOE.CREDENTIALS Users and administrators will set	NOE.CREDENTIALS ensures that users will not share their passwords, making it harder for

Threats	Objectives	Rationale
access to internal network resources.	secure passwords and will protect their access credentials.	an unauthorized person gain access to the TOE.
	NOE.INSTALL Those responsible for the TOE must ensure that the TOE is delivered, installed, managed, and operated in a manner which is consistent with common IT security policies. The TOE must be installed such that all traffic between the internal and external networks flows through it.	NOE.INSTALL ensures that the TOE will be installed correctly and configured securely. All traffic between the internal and external networks will flow through the TOE.
	NOE.MANAGE Sites deploying the TOE will provide competent, non-hostile TOE administrators who are appropriately trained and follow all administrator guidance. TOE administrators will ensure the system is used securely. The reliability of the TOE's timestamps will be ensured via periodic manual checks by the TOE administrator.	NOE.MANAGE ensures that the TOE will be managed by competent, non-hostile administrators who will configure the system securely to limit access to the TOE and who will periodically check the accuracy of the TOE's timestamps.
	O.INTACC The TOE must allow access to internal network resources only as defined by the VPN User Access Control SFP and the VPN User Information Flow Control SFP.	O.INTACC ensures that the TOE limits access to internal network resources to the authorized users.
	O.EXTACC The TOE must allow access to	O.EXTACC ensures that the TOE limits communications between itself and external IT entities

Threats	Objectives	Rationale
	external IT entities sending or receiving traffic through the TOE only as defined by the Web Application Firewall Information Flow Control SFP.	based on the Web Application Firewall rules.
	O.TIME The TOE must provide reliable timestamps for its own use.	O.TIME ensures that the TOE maintains the correct time to be used when the date and time are determining factors for access.
T.ACCESSTOE A user may gain unauthorized access to security data on the TOE.	O.ADMIN The TOE must include a set of functions that allow management of its functions and data, ensuring that TOE users with the appropriate privileges and only those TOE users, may exercise such control.	O.ADMIN ensures that only Administrators can access the management functions for the TOE.
	NOE.CREDENTIALS Users and administrators will set secure passwords and will protect their access credentials.	NOE.CREDENTIALS ensures that Administrators will not share their passwords, making it harder for an unauthorized person gain access to the TOE.
	O.AUDIT The TOE must record the actions taken by administrators (except actions performed at the underlying FreeBSD shell), prevent unauthorized deletion of the audit records stored on the TOE, and provide the authorized administrators with the ability to review the audit trail.	O.AUDIT ensures that events of security relevance (such as access to the TOE) are audited (except actions performed at the underlying FreeBSD shell).

Threats	Objectives	Rationale
	OE.EXTERNAL The TOE environment must ensure any authentication data in the environment are protected and maintained.	OE.EXTERNAL ensures that authentication data is stored securely outside of the TOE.
	NOE.INSTALL Those responsible for the TOE must ensure that the TOE is delivered, installed, managed, and operated in a manner which is consistent with common IT security policies. The TOE must be installed such that all traffic between the internal and external networks flows through it.	OE.INSTALL ensures that the TOE will be installed correctly and configured securely.
	O.AUTHENTICATE The TOE must be able to identify and authenticate administrators prior to allowing access to TOE administrative functions and data.	O.AUTHENTICATE ensures that Administrators identify and authenticate themselves before they are given access.
	NOE.MANAGE Sites deploying the TOE will provide competent, non-hostile TOE administrators who are appropriately trained and follow all administrator guidance. TOE administrators will ensure the system is used securely. The reliability of the TOE's timestamps will be ensured via periodic manual checks by the TOE administrator.	NOE.MANAGE ensures that the TOE will be managed by competent, non-hostile administrators who will configure the system securely to limit access to the TOE and who will periodically check the accuracy of the TOE's timestamps.

Threats	Objectives	Rationale
	O.TIME The TOE must provide reliable timestamps for its own use.	O.TIME ensures that the TOE has the correct time when recording audit records.
T.AVAIL An authorized user may not be able to utilize NetScaler services due to physical tampering of the TOE or the network.	NOE.AC The TOE environment must regulate the temperature of the facility where the TOE is located so no damage is caused by heat or cold.	NOE.AC ensures that the TOE's security mechanisms cannot be bypassed by tampering with the TOE environment's temperature.
	OE.CONNECT The TOE environment must provide network connectivity to the TOE. The network connection to the TOE must be reliable.	OE.CONNECT ensures that the TOE has a reliable network connection.
	NOE.PHYSICAL The physical environment must be suitable for supporting a computing device in a secure setting.	NOE.PHYSICAL ensures that the environment will protect the TOE from physical tampering.
	NOE.POWER The TOE environment must provide the electricity necessary to the TOE to function. The power to the TOE must be reliable and protected from surges and disconnects.	OE.POWER ensures that the TOE's security mechanisms cannot be bypassed by tampering with the electrical connection to the TOE.
T.MASQUERADE A user or process may masquerade as another entity in order to gain	NOE.CREDENTIALS Users and administrators will set secure passwords and will protect	NOE.CREDENTIALS ensures that Administrators will not share their passwords, making it harder for an unauthorized person to

Threats	Objectives	Rationale
unauthorized access to data or TOE resources.	their access credentials.	pretend to be an authorized Administrator.
	O.AUDIT The TOE must record the actions taken by administrators (except actions performed at the underlying FreeBSD shell), prevent unauthorized deletion of the audit records stored on the TOE, and provide the authorized administrators with the ability to review the audit trail.	O.AUDIT ensures that events of security relevance (such as Administrator login) are audited (except actions performed at the underlying FreeBSD shell).
	O.AUTHENTICATE The TOE must be able to identify and authenticate administrators prior to allowing access to TOE administrative functions and data.	O.AUTHENTICATE ensures that Administrators supply login credentials before being granted management access to the TOE.
T.MODCONF An attacker or unauthorized user may modify a user's configuration. This covers: modification of the user's set of permitted internal network resources modification of configuration data associated with a user.	O.AUDIT The TOE must record the actions taken by administrators (except actions performed at the underlying FreeBSD shell), prevent unauthorized deletion of the audit records stored on the TOE, and provide the authorized administrators with the ability to review the audit trail.	O.AUDIT ensures that events of security relevance (such as modification to a user's configuration) are audited (except actions performed at the underlying FreeBSD shell).
	OE.EXTERNAL The TOE environment must ensure any authentication data in the environment are protected and maintained.	OE.EXTERNAL ensures that that authentication data is stored securely outside of the TOE.

Threats	Objectives	Rationale
	O.AUTHENTICATE The TOE must be able to identify and authenticate administrators prior to allowing access to TOE administrative functions and data.	O.AUTHENTICATE ensures that Administrators identify and authenticate themselves before they are given access to configuration data.
	NOE.MANAGE Sites deploying the TOE will provide competent, non-hostile TOE administrators who are appropriately trained and follow all administrator guidance. TOE administrators will ensure the system is used securely. The reliability of the TOE's timestamps will be ensured via periodic manual checks by the TOE administrator.	NOE.MANAGE ensures that the TOE will be managed by competent, non-hostile administrators who will configure the system securely to limit access to the user's configuration data.
T.TAMPERING A user or process may be able to bypass the TOE's security mechanisms thereby compromising TOE user or system data.	NOE.AC The TOE environment must regulate the temperature of the facility where the TOE is located so no damage is caused by heat or cold.	NOE.AC ensures that the TOE's security mechanisms cannot be bypassed by tampering with the TOE environment's temperature.
	OE.CONNECT The TOE environment must provide network connectivity to the TOE. The network connection to the TOE must be reliable.	OE.CONNECT ensures that the TOE has a network connection.
	NOE.PHYSICAL The physical environment must be suitable for supporting a	NOE.PHYSICAL ensures that the environment will protect the TOE from physical tampering.

Threats	Objectives	Rationale
	computing device in a secure setting.	
	NOE.POWER The TOE environment must provide the electricity necessary to the TOE to function. The power to the TOE must be reliable and protected from surges and disconnects.	NOE.POWER ensures that the TOE's security mechanisms cannot be bypassed by tampering with the electrical connection to the TOE.

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.

8.4.2 Security Objectives Rationale Relating to Policies

There are no Organizational Security Policies defined. Therefore, there are no Security Objectives relating to Policies.

8.4.3 Security Objectives Rationale Relating to Assumptions

Table 14 introduces the assumptions to objectives mappings for the TOE.

Table 14 – Assumptions:Objectives Mapping

Assumptions	Objectives	Rationale
A.LOCATE The TOE is located within a controlled access facility which restricts physical access to the appliance to authorized persons only, and provides uninterruptible	OE.CONNECT The TOE environment must provide network connectivity to the TOE. The network connection to the TOE must be reliable.	OE.CONNECT ensures that the TOE has a reliable network connection.

Assumptions	Objectives	Rationale
power, air conditioning, and all other conditions required for reliable operation of the hardware.	NOE.AC The TOE environment must regulate the temperature of the facility where the TOE is located so no damage is caused by heat or cold.	NOE.AC ensures that the TOE's security mechanisms cannot be bypassed by tampering with the TOE environment's temperature.
A.NETCON The TOE environment provides the required network connectivity and the connectivity is protected from tampering. TOE Management will only be performed from the internal protected network.	OE.CONNECT The TOE environment must provide network connectivity to the TOE. The network connection to the TOE must be reliable.	OE.CONNECT ensures that the TOE has a reliable network connection.
A.DISCLOSE Users and administrators will not disclose their passwords.	NOE.CREDENTIALS Users and administrators will set secure passwords and will protect their access credentials.	NOE.CREDENTIALS ensures that users and Administrators will set secure passwords, making it harder for an unauthorized person gain access to the TOE.
A.EXTERNAL The external authentication servers are operating correctly and securely. Data transmitted between the TOE and the external servers is protected from tampering by un-trusted subjects during transfer to the external server, during storage on the external server, and during transmission to the TOE from the external server.	OE.EXTERNAL The TOE environment must ensure any authentication data in the environment are protected and maintained.	OE.EXTERNAL ensures that that authentication data will be kept secure outside of the TOE boundary.
A.LOCATE The TOE is located within a controlled access facility which	OE.EXTERNAL The TOE environment must ensure any authentication data in	OE.EXTERNAL ensures that that authentication data is stored securely outside of the TOE.

Assumptions	Objectives	Rationale
restricts physical access to the appliance to authorized persons only, and provides uninterruptible power, air conditioning, and all other conditions required for reliable operation of the hardware.	the environment are protected and maintained.	
A.NETCON The TOE environment provides the required network connectivity and the connectivity is protected from tampering. TOE Management will only be performed from the internal protected network.	OE.EXTERNAL The TOE environment must ensure any authentication data in the environment are protected and maintained.	OE.EXTERNAL ensures that that authentication data is stored securely outside of the TOE.
A.PASSWORDS Administrators and users will set passwords of at least eight characters that are not dictionary words or combinations of dictionary words, using a combination of uppercase, lowercase, numeric, and symbolic characters.	NOE.CREDENTIALS Users and administrators will set secure passwords and will protect their access credentials.	NOE.CREDENTIALS ensures that users and Administrators will set secure passwords, making it harder for an unauthorized person gain access to the TOE.
A.CRYPTO The TOE environment will ensure that the TOE stored cryptographic data is protected against tampering.	OE.CRYPTO The TOE environment must ensure that the stored cryptographic data is protected against tampering.	OE.CRYPTO ensures that the TOE environment will protect the stored cryptographic data against tampering.
A.INSTALL The TOE has been installed and configured according to the appropriate installation guides, and all traffic between the internal and	NOE.INSTALL Those responsible for the TOE must ensure that the TOE is delivered, installed, managed, and operated in a manner which is consistent with common IT	NOE.INSTALL ensures that the TOE will be installed correctly and configured securely. All traffic between the internal and external networks will flow through the TOE.

Assumptions	Objectives	Rationale
external networks flows through it.	security policies. The TOE must be installed such that all traffic between the internal and external networks flows through it.	
A.MANAGE There is one or more competent individual (administrator) assigned to manage the TOE and the security of the information it contains.	NOE.INSTALL Those responsible for the TOE must ensure that the TOE is delivered, installed, managed, and operated in a manner which is consistent with common IT security policies. The TOE must be installed such that all traffic between the internal and external networks flows through it.	NOE.INSTALL ensures that the TOE will be installed correctly and configured securely.
A.NOEVIL The users who manage the TOE are non-hostile, appropriately trained, and follow all guidance.	NOE.INSTALL Those responsible for the TOE must ensure that the TOE is delivered, installed, managed, and operated in a manner which is consistent with common IT security policies. The TOE must be installed such that all traffic between the internal and external networks flows through it.	NOE.INSTALL ensures that the TOE will be installed correctly and configured securely.
A.INSTALL The TOE has been installed and configured according to the appropriate installation guides, and all traffic between the internal and external networks flows through it.	NOE.MANAGE Sites deploying the TOE will provide competent, non-hostile TOE administrators who are appropriately trained and follow all administrator guidance. TOE administrators will ensure the system is used securely. The reliability of the TOE's timestamps will be ensured via periodic manual checks by the TOE	NOE.MANAGE ensures that the TOE will be managed by competent, non-hostile administrators who will configure the system securely to limit access to the user's configuration data.

Assumptions	Objectives	Rationale
	administrator.	
A.MANAGE There is one or more competent individual (administrator) assigned to manage the TOE and the security of the information it contains.	NOE.MANAGE Sites deploying the TOE will provide competent, non-hostile TOE administrators who are appropriately trained and follow all administrator guidance. TOE administrators will ensure the system is used securely. The reliability of the TOE's timestamps will be ensured via periodic manual checks by the TOE administrator.	NOE.MANAGE ensures that the TOE will be managed by competent, non-hostile administrators who will configure the system securely to limit access to the user's configuration data and who will periodically check the accuracy of the TOE's timestamps.
A.NOEVIL The users who manage the TOE are non-hostile, appropriately trained, and follow all guidance.	NOE.MANAGE Sites deploying the TOE will provide competent, non-hostile TOE administrators who are appropriately trained and follow all administrator guidance. TOE administrators will ensure the system is used securely. The reliability of the TOE's timestamps will be ensured via periodic manual checks by the TOE administrator.	NOE.MANAGE ensures that the TOE will be managed by competent, non-hostile administrators who will configure the system securely to limit access to the user's configuration data and who will periodically check the accuracy of the TOE's timestamps.
A.LOCATE The TOE is located within a controlled access facility which restricts physical access to the appliance to authorized persons only, and provides uninterruptible power, air conditioning, and all other conditions required for reliable operation of the hardware.	NOE.PHYSICAL The physical environment must be suitable for supporting a computing device in a secure setting.	NOE.PHYSICAL ensures that the TOE's environment is suitable for securely supporting the TOE.
	NOE.POWER The TOE environment must provide the electricity necessary	NOE.POWER ensures that the TOE's security mechanisms cannot be bypassed by tampering with the electrical connection to

Assumptions	Objectives	Rationale
	to the TOE to function. The power to the TOE must be reliable and protected from surges and disconnects.	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.

8.5 Rationale for Extended Security Functional Requirements

There are no extended security functional requirements defined.

8.6 Rationale for Extended TOE Security Assurance Requirements

There are no extended TOE security assurance requirements defined.

8.7 Security Requirements Rationale

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

8.7.1 Rationale for Security Functional Requirements of the TOE Objectives

Table 15 introduces the objectives to SFR mappings.

Table 15 – Objectives:SFRs Mapping

Objective	Requirements Addressing the Objective	Rationale

Objective	Requirements Addressing the Objective	Rationale
O.ADMIN The TOE must include a set of functions that allow management of its functions and data, ensuring that TOE users with the appropriate privileges and only those TOE users, may exercise such control.	FMT_MSA.3(a) Static attribute initialisation	FMT_MSA.3b defines static attribute initialization for the VPN User Access Control SFP and who can modify the default values.
	FDP_ACC.1(a) Subset access control	FDP_ACC.1a requires the TOE to enforce the Administrator Access Control SFP.
	FDP_ACF.1(a) Security attribute based access control	FDP_ACF.1a specifies the attributes used to enforce the Administrator Access Control SFP.
	FMT_MSA.1 Management of security attributes	FMT_MSA.1 specifies which roles can access security attributes.
	FMT_MSA.3(d) Static attribute initialisation	FMT_MSA.3(d) defines static attribute initialisation for the Web Application Firewall Information Flow Control SFP and who can modify the default values.
	FMT_MSA.3(c) Static attribute initialisation	FMT_MSA.3c defines static attribute initialization for the VPN User Information Flow Control SFP and who can modify the default values.
	FMT_MTD.1 Management of TSF data	FMT_MTD.1 specifies which roles can access TSF data.
	FMT_SMF.1 Specification of management functions	FMT_SMF.1 specifies the management functions the TOE must provide.

Objective	Requirements Addressing the Objective	Rationale
	FMT_SMR.1 Security roles	FMT_SMR.1 requires the TOE to maintain separate Administrator roles.
	FMT_MOF.1 Management of security functions behaviour	FMT_MOF.1 restricts access to TOE management functions.
O.AUDIT The TOE must record the actions taken by administrators (except actions performed at the underlying FreeBSD shell), prevent unauthorized deletion of the audit records stored on the TOE, and provide the authorized administrators with the ability to review the audit trail.	FAU_SAR.1 Audit review	FAU_SAR.1 requires that the TOE provide the authorized administrators with the ability to read the audit records.
	FAU_SAR.3 Selectable audit review	FAU_SAR.3 requires that the TOE provide the authorized administrators with the ability to search the audit records.
	FAU_STG.1 Protected audit trail storage	FAU_STG.1 requires that the TOE protect the audit records it holds.
	FAU_GEN.1 Audit data generation	FAU_GEN.1 requires that the TOE record all commands entered by an Administrator (except actions performed at the underlying FreeBSD shell).
O.AUTHENTICATE The TOE must be able to identify and authenticate administrators prior to allowing access to TOE administrative functions and data.	FIA_UAU.2 User authentication before any action	FIA_UAU.2 requires Administrators to be authenticated before they are able to perform any other actions.
	FIA_UID.2 User identification before any action	FIA_UID.2 requires Administrators to be identified before they are able to perform any other actions.

Objective	Requirements Addressing the Objective	Rationale
O.INTACC The TOE must allow access to internal network resources only as defined by the VPN User Access Control SFP and the VPN User Information Flow Control SFP.	FDP_IFF.1(a) Simple security attributes	FDP_IFF.1 specifies the attributes used to enforce the VPN Information Flow Control SFP.
	FDP_ACC.1(b) Subset access control	FDP_ACC.1b requires the TOE to enforce the VPN User Access Control SFP.
	FDP_ACF.1(b) Security attribute based access control	FDP_ACF.1b specifies the attributes used to enforce the VPN User Access Control SFP.
	FIA_UAU.2 User authentication before any action	FIA_UAU.2 requires VPN users to be authenticated before they are able to perform any other actions.
	FMT_MSA.3(b) Static attribute initialisation	FMT_MSA.3b defines static attribute initialization for the VPN User Access Control SFP and who can modify the default values.
	FDP_IFC.1(a) Subset information flow control	FDP_IFC.1 requires the TOE to enforce the VPN Information Flow Control SFP.
	FIA_UID.2 User identification before any action	FIA_UID.2 requires VPN users to be identified before they are able to perform any other actions.
O.EXTACC The TOE must allow access to external IT entities sending or receiving traffic through the TOE only as defined by the Web Application Firewall Information	FDP_IFF.1(b) Simple security attributes	FDP_IFF.1(b) specifies the attributes used to enforce the Web Application Firewall Information Flow Control SFP.
	FDP_IFC.1(b)	FDP_IFC.1(b) requires the TOE to enforce the Web Application

Objective	Requirements Addressing the Objective	Rationale
Flow Control SFP.	Subset information flow control	Firewall Information Flow Control SFP.
O.TIME The TOE must provide reliable timestamps for its own use.	FPT_STM.1 Reliable timestamps	FPT_STM.1 requires that the TOE provide reliable timestamps for its own use.

8.7.2 Security Assurance Requirements Rationale

EAL2 augmented with ALC_FLR.2 was chosen to provide a low to moderate level of assurance that is consistent with good commercial practices. As such, minimal additional tasks are placed upon the vendor assuming the vendor follows reasonable software engineering practices and can provide support to the evaluation for design and testing efforts. The chosen assurance level is appropriate with the threats defined for the environment. While the System may act as a gateway from a hostile environment, it is expected to be in a non-hostile position and embedded in or protected by other products designed to address threats that correspond with the intended environment. At EAL2 augmented with ALC_FLR.2, the System will have incurred a search for obvious flaws to support its introduction into the non-hostile environment.

The augmentation of ALC_FLR.2 was chosen to give greater assurance of the developer's on-going flaw remediation processes.

8.7.3 Dependency Rationale

This ST does satisfy all the requirement dependencies of the Common Criteria. Table 16 lists each requirement to which the TOE claims conformance with a dependency and indicates whether the dependent requirement was included. As the table indicates, all dependencies have been met.

Table 16 – Functional Requirements Dependencies

SFR ID	Dependencies	Dependency Met	Rationale

SFR ID	Dependencies	Dependency Met	Rationale
FAU_STG.1	FAU_GEN.1	✓	
FDP_IFC.1(b)	FDP_IFF.1(b)	✓	
FIA_UAU.2	FIA_UID.1	✓	Although FIA_UID.1 is not included, FIA_UID.2, which is hierarchical to FIA_UID.1, is included. This satisfies this dependency.
FDP_IFF.1(a)	FDP_IFC.1(a)	✓	
FDP_IFC.1(a)	FMT_MSA.3(a)	✓	
	FDP_IFF.1(a)	✓	
FDP_ACF.1(a)	FMT_MSA.3(a)	✓	
FMT_MOF.1	FMT_SMF.1	✓	
FDP_ACC.1(a)	FDP_ACF.1	✓	
FMT_MOF.1	FMT_SMR.1	✓	
FAU_SAR.3	FAU_SAR.1	✓	
FAU_SAR.1	FAU_GEN.1	✓	
FAU_GEN.1	FPT_STM.1	✓	
FMT_MSA.3(d)	FMT_SMR.1	✓	
	FMT_MSA.1	✓	
FDP_IFF.1(b)	FMT_MSA.3(d)	✓	
	FDP_IFC.1(b)	✓	

SFR ID	Dependencies	Dependency Met	Rationale
FDP_ACF.1(a)	FDP_ACC.1(a)	✓	
FMT_SMF.1	No dependencies	✓	
FDP_ACF.1(b)	FDP_ACC.1(b)	✓	
FDP_ACC.1(b)	FDP_ACF.1(b)	✓	
FMT_MSA.3(c)	FMT_SMR.1	✓	
	FMT_MSA.1	✓	
FMT_MSA.3(b)	FMT_SMR.1	✓	
	FMT_MSA.1	✓	
FIA_UID.2	No dependencies	✓	
FMT_SMR.1	FIA_UID.1	✓	Although FIA_UID.1 is not included, FIA_UID.2, which is hierarchical to FIA_UID.1, is included. This satisfies this dependency.
FDP_ACF.1(b)	FMT_MSA.3(b)	✓	
FMT_MTD.1	FMT_SMR.1	✓	
	FMT_SMF.1	✓	
FMT_MSA.3(a)	FMT_SMR.1	✓	
	FMT_MSA.1	✓	
FMT_MSA.1	FMT_SMR.1	✓	
	FMT_SMF.1	✓	

SFR ID	Dependencies	Dependency Met	Rationale
	FDP_ACC.1 or FDP_IFC.1	✓	FDP_ACC.1 and FDP_IFC.1 are included.
FPT_STM.1	No dependencies	✓	

9 Acronyms

9.1 Acronyms

Table 17 introduces the acronyms used throughout this document.

Table 17 – Acronyms

Acronym	Definition
CC	Common Criteria
CLI	Command Line Interface
CM	Configuration Management
DNS	Domain Name System
EAL	Evaluation Assurance Level
FIPS	Federal Information Processing Standard
FTP	File Transfer Protocol
GB	Gigabyte
Gbps	Gigabits per second
GUI	Graphical User Interface
HTTP	Hypertext Transfer Protocol
IP	Internet Protocol
IT	Information Technology
LCD	Liquid Crystal Display
LDAP	Lightweight Directory Access Protocol
Mbps	Megabits per second
NNTP	Network News Transfer Protocol
OS	Operating System
PP	Protection Profile
RADIUS	Remote Authentication Dial-In User Service
SAR	Security Assurance Requirement
SCP	Secure Copy
SFP	Security Functional Policy
SFP(t)	Small form-factor pluggable transceiver
SFR	Security Functional Requirement

Acronym	Definition
SFTP	Secure Shell File Transfer Protocol
SSH	Secure Shell
SSL	Secure Sockets Layer
ST	Security Target
TCP	Transmission Control Protocol
TOE	Target of Evaluation
TSF	TOE Security Function
TSP	TOE Security Policy
URL	Uniform Resource Locator
VPN	Virtual Private Network
WAN	Wide Area Network
XFP	10 Gigabit small form-factor pluggable transceiver

Prepared by:

Corsec Security, Inc.

10340 Democracy Lane, Suite 201
Fairfax, VA 22030

Phone: (703) 267-6050
Email: info@corsec.com
http://www.corsec.com