Citrix Systems, Inc.
NetScaler Application Switch with Access Gateway Enterprise Edition & Application Firewall Version 8.0

Security Target

Evaluation Assurance Level: EAL2 augmented with ALC_FLR.1
Document Version: 1.1

Prepared for:

Citrix Systems, Inc.
851 West Cypress Creek Road
Fort Lauderdale, FL 33309
United States of America
Phone: (954) 267-3000

http://www.citrix.com

Prepared by:

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

http://www.corsec.com

Revision History

Version	Modification Date	Modified By	Description of Changes
0.1	2007-09-24	Elizabeth Pugrud	Initial draft.
0.2	2007-12-20	Nathan Lee	Updates based on lab verdicts.
0.3	2008-02-26	Nathan Lee	Updates based on lab verdicts.
0.4	2008-03-12	Nathan Lee	Updates based on lab verdicts.
0.5	2008-05-02	Nathan Lee	Updates based on lab verdicts.
0.6	2008-05-30	Nathan Lee	Updates based on lab verdicts.
0.7	2008-06-18	Nathan Lee	Updates based on lab verdicts.
0.8	2008-06-18	Nathan Lee	Updates based on lab verdicts.
0.9	2008-07-13	Nathan Lee	Updates based on lab verdicts.
1.0	2008-07-15	Nathan Lee	Updates based on lab verdicts.
1.1	2008-07-16	Nathan Lee	Updated information on FreeBSD shell auditing.

Table of Contents

Table of Figures

Table of Tables

1 Security Target Introduction

This section identifies the Security Target (ST), Target of Evaluation (TOE), ST conventions, ST conformance claims, and the ST organization. The Target of Evaluation is the Citrix NetScaler Application Switch with Access Gateway Enterprise Edition & Application Firewall Version 8.0, and will hereafter be referred to as the TOE or the NetScaler throughout this document. The TOE is the NetScaler NS7000 and NS9010-FIPS appliances and all the installed firmware and software. The NetScaler is a purpose-built application performance accelerator.

1.1 Organization

This ST is divided into the following sections:

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

1.2 Security Target, TOE and CC Identification and Conformance

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

ST Title	Citrix Systems, Inc. NetScaler Application Switch with Access Gateway Enterprise Edition & Application Firewall Version 8.0 Security Target
ST Version	Version 1.1
Author	Corsec Security, Inc. Elizabeth Pugrud and Nathan Lee
TOE Identification	Citrix NetScaler Application Switch with Access Gateway Enterprise Edition & Application Firewall Version 8.0

Common Criteria Identification and Conformance	Common Criteria for Information Technology Security Evaluation (CC), Version 2.3, August 2005 (aligned with ISO/IEC 15408:2005); CC Part 2 conformant; CC Part 3 conformant; Parts 2 and 3 Interpretations from the Interpreted CC Evaluation Methodology as of October 1, 2007 were reviewed, and no interpretations apply to the claims made in this ST.
PP Identification	None
Evaluation Assurance Level	EAL2 augmented with ALC_FLR.1

1.3 Conventions, Acronyms, and Terminology

1.3.1 Conventions

There are several font variations used within this ST. Selected presentation choices are discussed here to aid the 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*.
- Completed selection statements are identified using <u>*underlined italicized text*</u>.
- Refinements are identified using **bold text**. Any text removed is stricken (Example: ~~TSF Data~~) and should be considered as a refinement.
- Iterations are identified by appending a letter in parentheses following the component title. For example, FAU_GEN.1(a) Audit Data Generation would be the first iteration and FAU_GEN.1(b) Audit Data Generation would be the second iteration.

1.3.2 Acronyms

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

2 TOE Description

The TOE Description provides an overview of the TOE. This section describes the general capabilities and security functionality of the TOE. The TOE Description provides a context for the TOE evaluation by identifying the product type, describing the product, and defining the specific evaluated configuration.

2.1 Product Type

The NetScaler Application Switch with Access Gateway Enterprise Edition & Application Firewall Version 8.0 is a dedicated application performance accelerator incorporating a Secure Sockets Layer (SSL) Virtual Private Network (VPN) with policy-based access control and an application-level firewall.

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

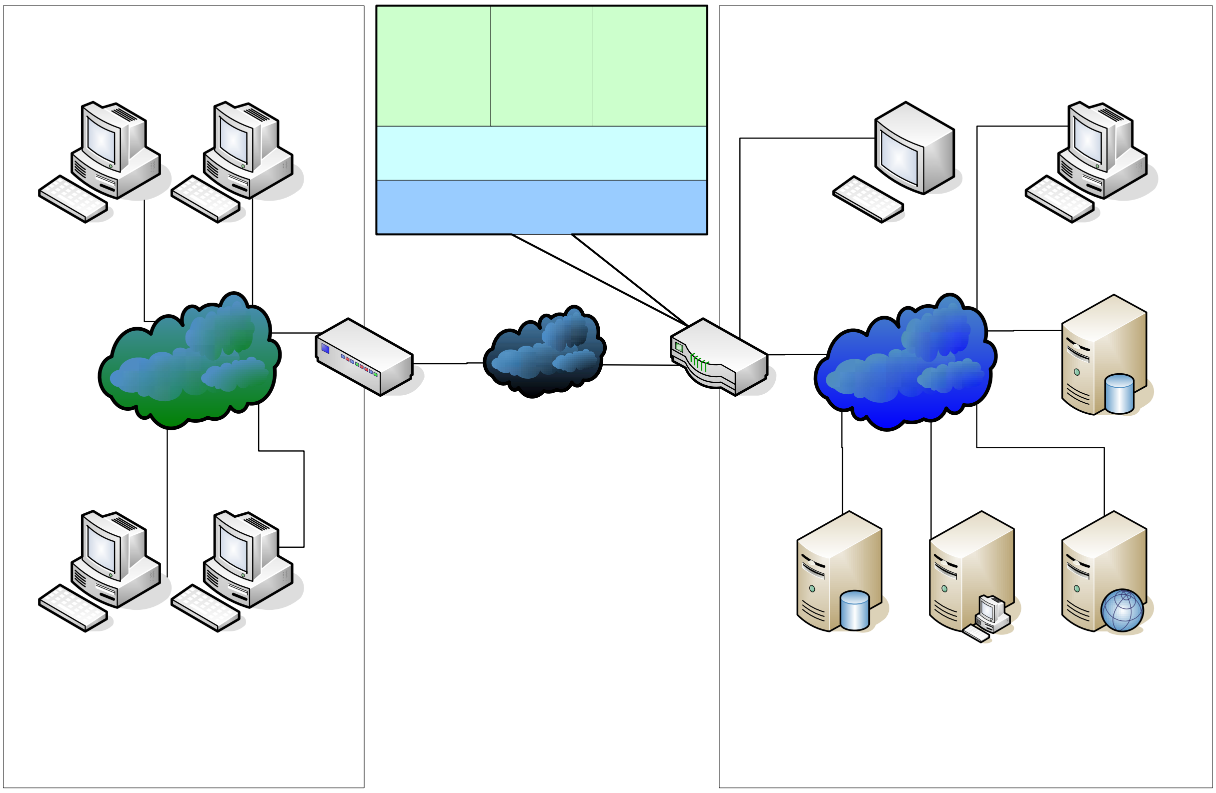

Figure 1 - Deployment Configuration of the TOE

2.2 Product Description

The NetScaler appliance incorporates three software components which work together to provide secure access to web-based applications, such as the Citrix Desktop Server or Presentation Server, from an external network. The three software components are the Application Switch, the Access Gateway and the Application Firewall. These run on top of the Application Delivery Networking Platform on the NetScaler NS7000 or NS9010-FIPS Appliance Hardware. These elements are described in the sections below.

TOE Administrators can access the TOE through a direct serial connection or from any workstation on the same network. 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. The NetScaler Configuration Utility is accessed via webbrowser.

2.2.1 Application Switch

The Application Switch component manages the connections between clients and servers. Clients establish a connection with the NetScaler rather than directly to a server. When the NetScaler receives application requests from the client, it establishes a connection with the appropriate application server. This allows the Application Switch 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. Additionally, it 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 Application Switch.

2.2.1.1 Load Balancing

The Load Balancing mechanism of the Application Switch allows the definition of Load Balancing virtual servers (vserver). Each Load Balancing vserver consists of an IP 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 physical 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 Application Switch supports protocol- and application-specific vservers for protocols such as HTTP, FTP, NNTP, and DNS.

2.2.1.2 Content Switching

The Content Switching mechanism of the Application Switch 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 Content Switching vserver determines which Load Balancing vserver to direct traffic to based on the content of the traffic. The Load Balancing vserver then directs the traffic to a physical server based on server load.

2.2.1.3 SSL Acceleration

The Application Switch component offers SSL Acceleration to relieve web servers of the burden of processing SSL transactions. The Application Switch 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. The NetScaler 9010-FIPS utilizes the NITROX XL CN1120-NFB Acceleration Board to provide FIPS 140-2-validated hardware-accelerated cryptographic functions.[1]

2.2.1.4 AppCache

The Application Switch 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] The NITROX XL CN1120-NFB Acceleration Board has FIPS 140-2 Cryptographic Module certificate #516.

2.2.1.5 AppCompress

The Application Switch can be configured to use the AppCompress, a feature that provides compression between the TOE and the end user. AppCompress uses the GZip compression algorithm, which yields up to 50% reduction in bandwidth requirements and improves end-user performance.

2.2.1.6 Surge Protection

Surge Protection within the Application Switch 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.

2.2.2 Access Gateway

The Access Gateway component is a 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.

2.2.3 Application Firewall

The 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. This model does not require the use of signatures and can protect against zero-day attacks.

2.2.4 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.

2.2.5 NS7000 and NS9010-FIPS Hardware Appliances

The NS7000 is a single processor unit that supports both Fast Ethernet and copper Gigabit Ethernet. The NS9010-FIPS supports Gigabit Ethernet over either fiber optic or copper cable. Both 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 two is the number of network ports available, the hardware performance, and the FIPS 140-2 Validated crypto card in the 9010-FIPS.

2.3 TOE Boundaries and Scope

This section will address what physical and logical components of the TOE are included in evaluation.

2.3.1 Physical Boundary

Figure 2 illustrates the physical scope and the physical boundary of the overall solution and ties together all of the components of the TOE and the constituents of the TOE Environment.

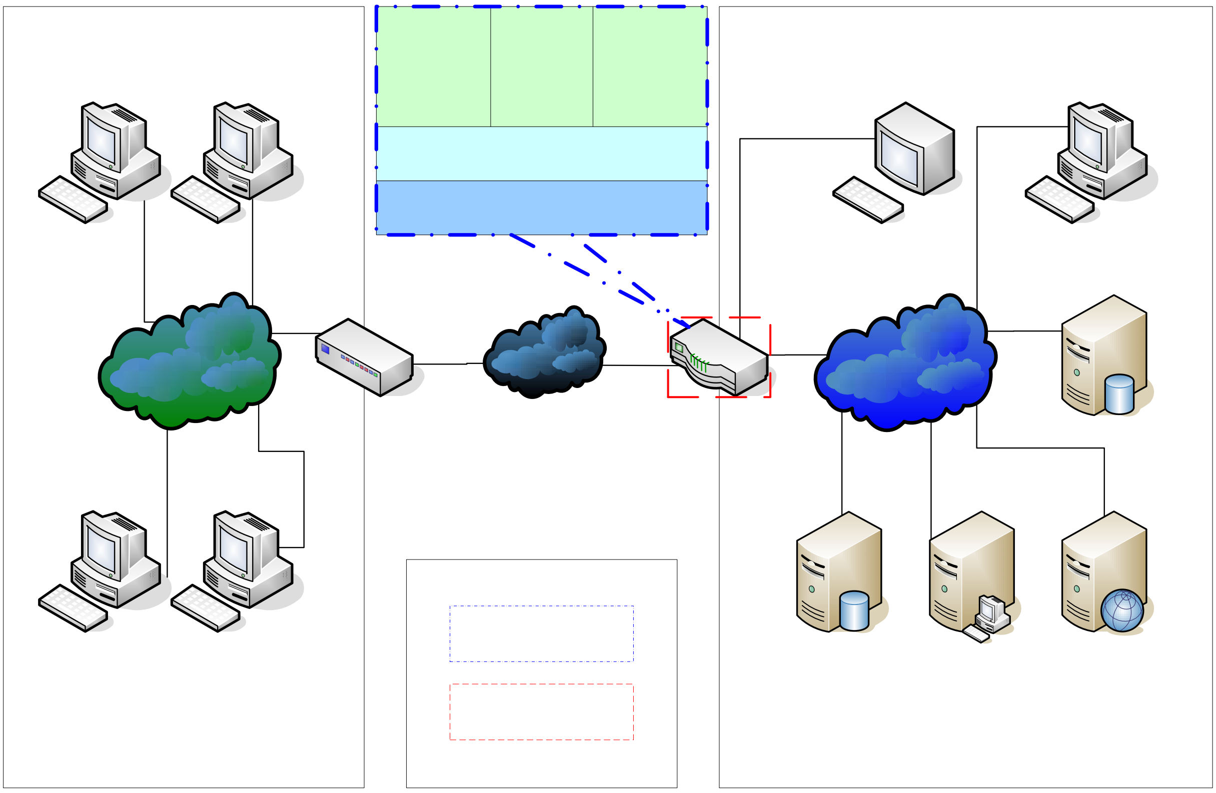

Figure 2 - TOE Boundary

The physical boundary of the TOE includes the NetScaler NS7000 and NS9010-FIPS Appliances as well as the firmware and software that run upon them.

2.3.1.1 TOE Environment

The TOE environment consists of the following:

- Administrator console and workstation for management
- Application server(s)
- VPN client(s)
- Network(s) (including the Internet and the Corporate Office Network)
- Authentication server (RADIUS[2], LDAP[3], TACACS+[4], or NT4)

2.3.2 Logical Boundary

User User

The logical boundary is shown in Figure 2 above. There are several logical components of the TOE: the NS7000 or NS9010-FIPS Appliance Hardware, the Application Delivery Networking Platform, the Application Switch

[2] Remote Authentication Dial In User Service

[3] Lightweight Directory Access Protocol

[4] Terminal Access Controller Access-Control System Plus

WA

Software, the Access Gateway Software, and the 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 greater detail below.

2.3.2.1 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.

2.3.2.2 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.

2.3.2.3 Identification and Authentication

Identification and authentication is performed against user information stored locally on the TOE or user information stored on an external Active Directory, RADIUS, LDAP, TACACS+, or NT4 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.

2.3.2.4 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 role grants them access.

2.3.2.5 Protection of the TSF

The TOE protects itself by providing a domain for its own execution that cannot be accessed by untrusted subjects, and by ensuring that the TSFs cannot be bypassed. A TOE execution domain is provided by a combination of physical protection of the TOE, a TSF that prevents access by unauthorized users, and lack of visibility to non-TOE devices, users, or entities on the systems being monitored. Non-bypassability of the TSFs is provided by preventing unauthorized users to access the TOE and by role enforcement. The TOE provides a reliable time stamp mechanism for its own use.

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

No product features or functionality are excluded from the evaluated configuration of the TOE.

3 Security Environment

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

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

3.1 Assumptions

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 2 - Assumptions

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.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.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.NOEVIL	The users and administrators of the TOE are non-hostile, appropriately trained, and follow all guidance.
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 untrusted subjects both during transfer to the external server, during storage on the external server, and during transmission to the TOE from the external server.
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.
A.DISCLOSE	Users and administrators will not disclose their passwords.

3.2 Threats to Security

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

- Attackers who are not TOE users: They have public knowledge of how the TOE operates and are assumed to possess a low skill level, limited resources to alter TOE configuration settings and parameters, no physical access to the TOE, and low motivation to attack the TOE.
- TOE users: This includes both VPN users and Administrators. They have extensive knowledge of how the TOE operates and are assumed to possess a high skill level, moderate resources to alter TOE configuration settings and parameters and physical access to the TOE. However, it is assumed that TOE users are not willfully hostile to the TOE.

The IT assets requiring protection are the hosts on the protected network. Removal, diminution and mitigation of the threats are through the objectives identified in Section 4 – Security Objectives.

This Security Target focuses on the security of the TOE administrative interfaces. The TOE provides many features which focus on protecting user data, but the security of these features is beyond the scope of this evaluation. The following threats are applicable to the TOE:

Table 3 - Threats

Threat 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.TAMPERING	An unauthorized user or process may be able to bypass the TOE’s security mechanisms by tampering with the TOE or TOE environment.
T.ACCESSTOE	A user may gain unauthorized access to security data on the TOE.
T.ACCESSINT	A user may gain unauthorized access to internal network 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.AVAIL	An authorized user may not be able to utilize NetScaler services due to physical tampering of the TOE or the network.

3.3 Organizational Security Policies

There are no Organizational Security Policies that apply to the TOE.

4 Security Objectives

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

4.1 Security Objectives for the TOE

The specific security objectives for the TOE are as follows:

Table 4 - Security Objectives for the TOE

Objective Name	Description
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.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.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.TIME	The TOE must provide reliable timestamps for its own use.
O.AUTHENTICATE	The TOE must be able to identify and authenticate administrators prior to allowing access to TOE administrative functions and data.
O.PROTECT	The TOE must ensure the integrity of audit and system data by protecting itself from unauthorized modifications and access to its functions and data.

4.2 Security Objectives for the Environment

4.2.1 IT Security Objectives

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

Table 5 - Objectives for the IT Environment

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.

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 6 - Objectives for the non-IT Environment

Name	Description
OE.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.
OE.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.PHYSICAL	The physical environment must be suitable for supporting a computing device in a secure setting.
OE.CREDENTIALS	Users and administrators will set secure passwords and will protect their access credentials.
OE.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.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.

5 Security Requirements

This section defines the Security Functional Requirements and Security Assurance Requirements (SARs) met by the TOE as well as Security Functional Requirements met by the TOE IT environment. These requirements are presented following the conventions identified in Section 1.3.1.

5.1 TOE Security Functional Requirements

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

Table 7 - TOE Security Functional Requirements

SFR Short Name	SFR Long Name	CC Operations			
		Selection	Assignment	Refinement	Iteration
FAU_GEN.1	Audit Data Generation	✓	✓		
FAU_SAR.1	Audit review		✓		
FAU_SAR.3	Selectable audit review	✓	✓		
FAU_STG.1	Protected audit trail storage	✓			
FDP_ACC.1	Subset access control		✓		✓
FDP_ACF.1	Security attribute based access control		✓		✓
FDP_IFC.1	Subset information flow control		✓		
FDP_IFF	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	Static attribute initialisation	✓	✓		✓

SFR Short Name	SFR Long Name	CC Operations			
		Selection	Assignment	Refinement	Iteration
FMT_MTD.1	Management of TSF data	✓	✓		
FMT_SMF.1	Specification of management functions		✓		
FMT_SMR.1	Security roles		✓		
FPT_RVM.1	Non-bypassability of the TSP[5]				
FPT_SEP.1	TSF domain separation				
FPT_STM.1	Reliable Timestamps				

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

[5] TOE Security Policy

5.1.1 Class FAU: Security Audit

FAU_GEN.1 Audit Data Generation

Hierarchical to: No other components.

FAU_GEN.1.1

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

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

b) All auditable events, for the *not specified*[6] level of audit; and

c) *all administrator executed commands (including failed login attempts, except commands executed at the underlying FreeBSD shell).*

FAU_GEN.1.2

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

a) Date and time of the event, type of event, subject identity, and the outcome (success or failure) of the event; and

b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, *the IP address of the user*.

Dependencies: FPT_STM.1 Reliable time stamps

Application Note: When adding a new system user, the audit log may contain the initial password for the new user in plaintext. The administrator should ensure that the audit logs are protected from viewing and tampering by untrusted subjects.

FAU_SAR.1 Audit review

Hierarchical to: No other components.

FAU_SAR.1.1

The TSF shall provide *read-only, network, operator, 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.

Dependencies: FAU_GEN.1 Audit data generation

[6] There is only one level of audit.

FAU_SAR.3 Selectable audit review

Hierarchical to: No other components.

FAU_SAR.3.1

The TSF shall provide the ability to perform *searches* of audit data based on *keywords through the CLI*.

Dependencies: FAU_SAR.1 Audit review

FAU_STG.1 Protected audit trail storage

Hierarchical to: No other components.

FAU_STG.1.1

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

FAU_STG.1.2

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

Dependencies: FAU_GEN.1 Audit data generation

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.

5.1.2 Class FDP: User Data Protection

FDP_ACC.1a Subset access control – Administrator Access Control

Hierarchical to: No other components.

FDP_ACC.1.1a

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

- *Subjects:*
  - i. *Administrators*
- *Objects:*
  - i. *Commands*
- *Operations:*
  - i. *Execute*

Dependencies: FDP_ACF.1 Security attribute based access control

FDP_ACC.1b Subset access control – VPN Access Control

Hierarchical to: No other components.

FDP_ACC.1.1b

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

- *Subjects:*
  - i. *VPN Clients*
- *Objects:*
  - i. *VPN connections*
- *Operations:*
  - i. *Establish*
  - ii. *Disconnect*

Dependencies: FDP_ACF.1 Security attribute based access control

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

Hierarchical to: No other components.

FDP_ACF.1.1a

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

- *Subjects:*
  - *i. Administrators*
- *Subject Attributes:*
  - *i. Roles assigned to administrators or assigned to an administrator’s group*

- *Objects:*
    i. *Commands*
- *Object Attributes:*
    i. *None*

FDP_ACF.1.2a

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.1.3a

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

- *All administrators are given execute permission to the commands "help", "show license", "set cli mode", and "set cli prompt".*

FDP_ACF.1.4a

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.*

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

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

Hierarchical to: No other components.

FDP_ACF.1.1b

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

- *Subjects:*
  - i. *VPN Clients*
- *Subject Attributes:*
  - i. *Username*
  - ii. *Password*
  - iii. *SSL Certificate attributes*
  - iv. *Source IP*[7] *address and/or subnet mask*
- *Objects:*
  - i. *VPN Connections*
- *Object Attributes:*
  - i. *Day and time accessible*

FDP_ACF.1.2b

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.*
- *Else, the user is denied establish.*
- *A user is given disconnect to a VPN connection only if he is the owner of the VPN connection.*

FDP_ACF.1.3b

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

- *No additional rules.*

FDP_ACF.1.4b

The TSF shall explicitly deny access of subjects to objects based on the

- *No additional rules.*

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

FDP_IFC.1 Subset information flow control

Hierarchical to: No other components.

FDP_IFC.1.1

[7] Internet Protocol

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

- *Subjects:*
  - *i. VPN Clients*
- *Information:*
  - *i. Internal Network Resources*
- *Operation:*
  - *i. Access*

Dependencies: FDP_IFF.1 Simple security attributes

FDP_IFF.1 Simple security attributes

Hierarchical to: No other components.

FDP_IFF.1.1

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

- *Subjects:*
  - *i. VPN Clients*
- *Subject Attributes:*
  - *i. Username*
  - *ii. Group*
- *Information:*
  - *i. Internal Network Resources*
- *Information Attributes:*
  - *Server IP address and port number*
  - *Intranet domain*

FDP_IFF.1.2

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

- *The 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

The TSF shall enforce the

- *no additional information flow control SFP rules.*

FDP_IFF.1.4

The TSF shall provide the following

- *no additional SFP capabilities.*

FDP_IFF.1.5

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

- *no additional rules.*

FDP_IFF.1.6

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

- *no additional rules.*

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

5.1.3 Class FIA: Identification and Authentication

FIA_UAU.2 User authentication before any action

Hierarchical to: FIA_UAU.1

FIA_UAU.2.1

The TSF shall require each user 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

FIA_UID.2.1

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

Dependencies: No dependencies

5.1.4 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 8 – FMT Access Control Matrix

Role / User 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	Create, delete, query, modify	Create, delete, query, modify	Create, delete, query, modify	As defined
VPN user permissions	Query	Create, delete, 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
Audit	Determine the behaviour of	Determine the behaviour of	Determine the behaviour of	Determine the behaviour of, modify the behaviour of	As defined
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

Note regarding Access Control Matrix: "nsroot" is the only account allowed to access the Audit data via SFTP or SCP protocols – all other accounts, even the superuser account, will be denied access.

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* **as specified in Table 8 above** the functions *listed in Table 8 above* to *the administrator roles listed in Table 8 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 *Administrator Access Control SFP* to restrict the ability to *query, modify, delete, or create as specified in Table 8 above* the security attributes *listed in Table 8 above* to *the administrator roles listed in Table 8 above*.

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

FMT_MSA.3a Static attribute initialisation – Administrator Access Control SFP

Hierarchical to: No other components.

FMT_MSA.3.1a

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

FMT_MSA.3.2a

The TSF shall allow the *superuser and authorized 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.3b Static attribute initialisation – VPN Access Control SFP

Hierarchical to: No other components.

FMT_MSA.3.1b

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.3.2b

The TSF shall allow the *operator, network, superuser, and authorized 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.3c Static attribute initialisation – VPN Information Flow Control SFP

Hierarchical to: No other components.

FMT_MSA.3.1c

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.3.2c

The TSF shall allow the *operator, network, superuser, and custom authorized 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 8* above the *TSF data listed in Table 8 above* to *the administrator roles listed in Table 8 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*

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, super user, 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

5.1.5 Class FPT: Protection of the TSF

FPT_RVM.1 Non-bypassability of the TSP

Hierarchical to: No other components.

FPT_RVM.1.1

The TSF shall ensure that TSP enforcement functions are invoked and succeed before each function within the TSC[8] is allowed to proceed.

Dependencies: No dependencies

FPT_SEP.1 TSF domain separation

Hierarchical to: No other components.

FPT_SEP.1.1

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

FPT_SEP.1.2

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

Dependencies: No dependencies

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

[8] TOE Scope of Control

5.2 Security Functional Requirements on the IT Environment

The TOE has the following security requirements for its IT environment:

Table 9 - SFRs for the IT Environment

Name	Description	S	A	R	I
FIA_UAU.3	Unforgeable authentication	✓		✓	

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

FIA_UAU.3 Unforgeable authentication

Hierarchical to: No other components.

FIA_UAU.3.1

The ~~TSF~~ **IT Environment** shall [*prevent*] use of authentication data that has been forged by any user of the TSF.

FIA_UAU.3.2

The ~~TSF~~ **IT Environment** shall [*prevent*] use of authentication data that has been copied from any other user of the TSF.

Dependencies: No dependencies

5.3 Assurance Requirements

This section defines the assurance requirements for the TOE. Assurance requirements are taken from the CC Part 3 and are EAL2 augmented with ALC_FLR.1. Table 10 – Assurance Requirements summarizes the requirements.

Table 10 – Assurance Requirements

Assurance Requirements	
Class ACM: Configuration management	ACM_CAP.2 Configuration items
Class ADO: Delivery and operation	ADO_DEL.1 Delivery procedures
	ADO_IGS.1 Installation, generation, and start-up procedures
Class ADV: Development	ADV_FSP.1 Informal functional specification

Assurance Requirements	
	ADV_HLD.1 Descriptive high-level design
	ADV_RCR.1 Informal correspondence demonstration
Class AGD: Guidance documents	AGD_ADM.1 Administrator guidance
	AGD_USR.1 User guidance
Class ALC : Life Cycle Support	ALC_FLR.1 Basic Flaw Remediation
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_SOF.1 Strength of TOE security function evaluation
	AVA_VLA.1 Developer vulnerability analysis

6 TOE Summary Specification

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

6.1 TOE Security Functions

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

Table 11 – Mapping of TOE Security Functions to Security Functional Requirements

TOE Security Function	TSF Subpart	SFR
Security Audit	Security_Audit-1	FAU_GEN.1
	Security_Audit-2	FAU_STG.1
	Security_Audit-3	FAU_SAR.1 FAU_SAR.3 FMT_MTD.1 FMT_SMF.1
User Data Protection	Admin_AC-1	FDP_ACC.1a
	Admin_AC-2	FDP_ACF.1a
	Admin_AC-3	FDP_ACF.1a
	VPN_AC-1	FDP_ACC.1b
	VPN_AC-2	FDP_ACF.1b FIA_UAU.2 FIA_UID.2
	VPN_AC-3	FDP_ACF.1b
	VPN_IFC-1	FDP_IFC.1
	VPN_IFC-2	FDP_IFF.1
Identification and Authentication	IA-1	FIA_UAU.2 FIA_UID.2

TOE Security Function	TSF Subpart	SFR
Security Management	Security_Management-1	FMT_SMR.1
	Security_Management-2	FMT_MOF.1 FMT_MSA.1 FMT_MTD.1
	Security_Management-3	FMT_SMF.1
	Security_Management-4	FMT_MSA.3a FMT_MSA.3b FMT_MSA.3c
Protection of TOE Security Functions	TSF_Protection-1	FPT_RVM.1
	TSF_Protection-2	FPT_SEP.1
	TSF_Protection-3	FPT_STM.1

6.1.1 Security Audit

- Security_Audit-1: 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 (except commands executed at the underlying FreeBSD shell). 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, and the exact command (with selected options) that the administrator attempted to execute and indication of the success or failure of the command. (FAU_GEN.1)

- Security_Audit-2: 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 superuser or a custom allowed role) can read or delete them. (FAU_STG.1)

- Security_Audit-3: 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. (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.3, FAU_STG.1, FMT_MTD.1, and FMT_SMF.1.

6.1.2 User Data Protection

The TOE enforces the following SFPs:

6.1.2.1 Administrator Access Control SFP

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

- Admin_AC-2: Administrators are assigned roles or are members of groups which 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.1a)

- Admin_AC-3: 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 commands "help", "show ns info", and "set lb vserver".
    - 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.1a)

6.1.2.2 VPN Access Control SFP

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

- VPN_AC-2: Users can be authenticated based on their username, password, client SSL certificate attributes, source IP and/or netmask, and/or 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.1b, FIA_UAU.2, FIA_UID.2)

- VPN_AC-3: The user may terminate the connection by logging out or closing the VPN window. A user can disconnect only his VPN connection. (FDP_ACF.1b)

6.1.2.3 VPN Information Flow Control SFP

- VPN_IFC-1: 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)

- VPN_IFC-2: Which resources are accessible to each user are configured by the administrator. 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)

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

6.1.3 Identification and Authentication

- IA-1: 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, LDAP, TACACS+, or NT4 Server. (FIA_UAU.2, FIA_UID.2)

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

6.1.4 Security Management

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

- Security_Management-2: 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 8 above. (FMT_MOF.1, FMT_MSA.1, FMT_MTD.1)

- Security_Management-3: 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. (FMT_SMF.1)

- Security_Management-4: The TOE also manages the SFPs discussed in Section 6.1.2 above 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.3a, FMT_MSA.3b, FMT_MSA.3c)

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

6.1.5 Protection of the TSF

- TSF_Protection-1: The TOE is self contained; the hardware, firmware, and software provide all the services necessary to implement the supported TSFs. No general purpose operating system, programming interfaces, or external disk storage is provided. The CLI and NetScaler Configuration Utility restrict administrators to a specific set of commands for modifying the configuration and data of the TOE. The configuration or data cannot be directly modified without violating the physical security of the NetScaler hardware (part of the TOE Environment). An underlying assumption of the TOE environment is that it will maintain the physical security of the TOE. Thus, the TSP enforcement functions are invoked and succeed before each function within the TSC is allowed to proceed. (FPT_RVM.1)

- TSF_Protection-2: The Application Delivery Networking Platform controls the execution of each process and ensures that all the information used for management purposes is protected from direct access by any other process. Furthermore, in order to ensure the correct execution of each process, the Application Delivery Networking Platform protects each process's private information (executable code, data, and stack) from uncontrolled interferences from other processes. These features ensure that the TSF maintains a security domain for its own execution that protects it from interference and tampering by untrusted subjects and enforces separation between the security domains of Administrators. (FPT_SEP.1)
- TSF_Protection-3: 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_RVM.1, FPT_SEP.1, and FPT_STM.1.

6.2 TOE Security Assurance Measures

EAL2 augmented with ALC_FLR.1 was chosen to provide a basic level of independently assured security. This section of the Security Target maps the assurance requirements of the TOE for a CC EAL2 augmented with ALC_FLR.1 level of assurance to the assurance measures used for the development and maintenance of the TOE. The following table provides a mapping of the appropriate documentation to the TOE assurance requirements.

Note to Evaluator: The final versions of these documents have not yet been produced. The version numbers will be completed when the evaluation is close to completion and the documents have been finalized.

Table 12 - Assurance Measures Mapping to TOE Security Assurance Requirements (SARs)

Assurance Component	Assurance Measure
ACM_CAP.2	Citrix NetScaler Application Switch with Access Gateway Enterprise Edition & Application Firewall Version 8.0 - Configuration Management
ADO_DEL.1	Citrix NetScaler Application Switch with Access Gateway Enterprise Edition & Application Firewall Version 8.0 - Secure Delivery
ADO_IGS.1	Quick Installation and Configuration NetScaler Application Switch Installation and Configuration Guide – Vol. 1 Citrix Access Gateway Enterprise Edition Quick Start Guide
ADV_FSP.1	Citrix NetScaler Application Switch with Access Gateway Enterprise Edition & Application Firewall Version 8.0 - TOE Architecture: High Level Design, Functional Specification, and Representation Correspondence

Assurance Component	Assurance Measure
ADV_HLD.1	Citrix NetScaler Application Switch with Access Gateway Enterprise Edition & Application Firewall Version 8.0 - TOE Architecture: High Level Design, Functional Specification, and Representation Correspondence
ADV_RCR.1	Citrix NetScaler Application Switch with Access Gateway Enterprise Edition & Application Firewall Version 8.0 - TOE Architecture: High Level Design, Functional Specification, and Representation Correspondence
AGD_ADM.1	NetScaler Application Switch Installation and Configuration Guide – Vol. 1 NetScaler Application Switch Installation and Configuration Guide – Vol. 2 Citrix Application Firewall Guide Release 8.0 Citrix® Access Gateway Enterprise Edition Administrator’s Guide Citrix NetScaler Application Switch Command Reference Guide
AGD_USR.1	Access Gateway Enterprise Edition User’s Guide for the Windows® Platform Release 8.0 Access Gateway Enterprise Edition User’s Guide for the Windows®, Mac OS, Linux, and Unix Platforms Release 8.0 SSL VPN User’s Guide for the Windows® Platform Release 8.0 SSL VPN User’s Guide for the Windows®, Mac OS, Linux, and Unix Platforms Release 8.0
ALC_FLR.1	Citrix NetScaler Application Switch with Access Gateway Enterprise Edition & Application Firewall Version 8.0 – Life Cycle Support: Flaw Remediation
ATE_COV.1	Citrix NetScaler Application Switch with Access Gateway Enterprise Edition & Application Firewall Version 8.0 – Functional Tests and Coverage
ATE_FUN.1	Citrix NetScaler Application Switch with Access Gateway Enterprise Edition & Application Firewall Version 8.0 – Functional Tests and Coverage
AVA_SOF.1	Citrix NetScaler Application Switch with Access Gateway Enterprise Edition & Application Firewall Version 8.0 - Vulnerability Assessment
AVA_VLA.1	Citrix NetScaler Application Switch with Access Gateway Enterprise Edition & Application Firewall Version 8.0 - Vulnerability Assessment

7 Protection Profile Claims

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

7.1 Protection Profile Reference

There are no protection profile claims for this security target.

8 Rationale

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

8.1 Security Objectives Rationale

This section provides a rationale for the existence of each assumption, threat, and policy statement that compose the Security Target. Table 13 demonstrates the mapping from the assumptions, threats, and polices to the security objectives is complete. The following discussion provides detailed evidence of coverage for each assumption, threat, and policy.

Table 13 - Mapping of Security Objectives to Threats, Policies, and Assumptions

Objectives Threats Policies Assumptions	O.AUDIT	O.INTACC	O.ADMIN	O.TIME	O.AUTHENTICATE	O.PROTECT	OE.CONNECT	OE.POWER	OE.AC	OE.EXTERNAL	OE.MANAGE	OE.INSTALL	OE.PHYSICAL	OE.CREDENTIALS
THREATS														
T.MASQUERADE	✓				✓									✓
T.TAMPERING						✓	✓	✓	✓				✓	
T.ACCESSTOE	✓		✓	✓	✓					✓	✓	✓		✓
T.ACCESSINT		✓		✓							✓	✓		✓
T.MODCONF	✓				✓	✓				✓	✓			
T.AVAIL						✓	✓	✓	✓				✓	
POLICIES														
ASSUMPTIONS														
A.INSTALL											✓	✓		
A.NETCON							✓			✓				
A.LOCATE							✓	✓	✓	✓			✓	

Objectives Threats Policies Assumptions	O.AUDIT	O.INTACC	O.ADMIN	O.TIME	O.AUTHENTICATE	O.PROTECT	OE.CONNECT	OE.POWER	OE.AC	OE.EXTERNAL	OE.MANAGE	OE.INSTALL	OE.PHYSICAL	OE.CREDENTIALS
A.MANAGE											✓	✓		
A.NOEVIL											✓	✓		
A.EXTERNAL										✓				
A.PASSWORDS														✓
A.DISCLOSE														✓

8.1.1 Security Objectives Rationale Relating to Threats

Table 14 - Threats-Objectives Mapping

Threats	Objectives	Rationale
T.MASQUERADE A user or process may masquerade as another entity in order to gain unauthorized access to data or TOE resources.	O.AUDIT	O.AUDIT ensures that events of security relevance (such as Administrator login) are audited (except actions performed at the underlying FreeBSD shell).
	O.AUTHENTICATE	O.AUTHENTICATE ensures that Administrators supply login credentials before being granted management access to the TOE.
	OE.CREDENTIALS	OE.CREDENTIALS ensures that Administrators will not share their passwords, making it harder for an unauthorized person to pretend to be an authorized Administrator.
T.TAMPERING An unauthorized user or process may be able to bypass the TOE's security mechanisms by tampering with the TOE or TOE environment.	O.PROTECT	O.PROTECT ensures that the protection mechanisms of the TOE designed to prevent tampering with TOE IT assets are in place and functioning properly, and that these mechanisms cannot be bypassed
	OE.CONNECT	OE.CONNECT ensures that the TOE has a network connection.
	OE.POWER	OE.POWER ensures that the TOE's security mechanisms cannot be bypassed by tampering with the electrical connection to the TOE.

Threats	Objectives	Rationale
	OE.AC	OE.AC ensures that the TOE's security mechanisms cannot be bypassed by tampering with the TOE environment's temperature.
	OE.PHYSICAL	OE.PHYSICAL ensures that the environment will protect the TOE from physical tampering.
T.ACCESSTOE A user may gain unauthorized access to security data on the TOE.	O.AUDIT	O.AUDIT ensures that events of security relevance (such as access to the TOE) are audited (except actions performed at the underlying FreeBSD shell).
	O.ADMIN	O.ADMIN ensures that only Administrators can access the management functions for the TOE.
	O.TIME	O.TIME ensures that the TOE has the correct time when recording audit records.
	O.AUTHENTICATE	O.AUTHENTICATE ensures that Administrators identify and authenticate themselves before they are given access.
	OE.EXTERNAL	OE.EXTERNAL ensures that authentication data is stored securely outside of the TOE.
	OE.MANAGE	OE.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.
	OE.INSTALL	OE.INSTALL ensures that the TOE will be installed correctly and configured securely.
	OE.CREDENTIALS	OE.CREDENTIALS ensures that Administrators will not share their passwords, making it harder for an unauthorized person gain access to the TOE.
T.ACCESSINT A user may gain unauthorized access to internal network resources.	O.INTACC	O.INTACC ensures that the TOE limits access to internal network resources to the authorized users.
	O.TIME	O.TIME ensures that the TOE maintains the correct time to be used when the date and time are determining factors for access.
	OE.MANAGE	OE.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
	OE.INSTALL	OE.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.
	OE.CREDENTIALS	OE.CREDENTIALS ensures that users will not share their passwords, making it harder for an unauthorized person gain 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	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).
	O.AUTHENTICATE	O.AUTHENTICATE ensures that Administrators identify and authenticate themselves before they are given access to configuration data.
	OE.EXTERNAL	OE.EXTERNAL ensures that that authentication data is stored securely outside of the TOE.
	OE.MANAGE	OE.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.
	O.PROTECT	O.PROTECT ensures that the TOE protects user configuration data from unauthorized modifications.
T.AVAIL An authorized user may not be able to utilize NetScaler services due to physical tampering of the TOE or the network.	O.PROTECT	O.PROTECT ensures that the protection mechanisms of the TOE designed to prevent tampering with TOE IT assets are in place and functioning properly, and that these mechanisms cannot be bypassed.
	OE.CONNECT	OE.CONNECT ensures that the TOE has a reliable network connection.
	OE.POWER	OE.POWER ensures that the TOE's security mechanisms cannot be bypassed by tampering with the electrical connection to the TOE.
	OE.AC	OE.AC ensures that the TOE's security mechanisms cannot be bypassed by tampering with the TOE environment's temperature.
	OE.PHYSICAL	OE.PHYSICAL ensures that the environment will protect the TOE from physical tampering.

8.1.2 Security Objectives Rationale Relating to Policies

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

8.1.3 Security Objectives Rationale Relating to Assumptions

Table 15 - Assumptions-Objectives Mapping

Assumptions	Objectives	Rationale
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.	OE.MANAGE	OE.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.
	OE.INSTALL	OE.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.
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	OE.CONNECT ensures that the TOE has a reliable network connection.
	OE.EXTERNAL	OE.EXTERNAL ensures that that authentication data is stored securely outside of the TOE.
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.	OE.CONNECT	OE.CONNECT ensures that the TOE has a reliable network connection.
	OE.POWER	OE.POWER ensures that the TOE's security mechanisms cannot be bypassed by tampering with the electrical connection to the TOE.
	OE.AC	OE.AC ensures that the TOE's security mechanisms cannot be bypassed by tampering with the TOE environment's temperature.
	OE.EXERNAL	OE.EXTERNAL ensures that that authentication data is stored securely outside of the TOE.
	OE.PHYSICAL	OE.PHYSICAL ensures that the TOE's environment is suitable for securely supporting the TOE.
A.MANAGE There is one or more competent individual (administrator) assigned to manage the TOE and the security of the information it	OE.MANAGE	OE.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.

Assumptions	Objectives	Rationale
contains.	OE.INSTALL	OE.INSTALL ensures that the TOE will be installed correctly and configured securely.
A.NOEVIL The users and administrators of the TOE are non-hostile, appropriately trained, and follow all guidance.	OE.MANAGE	OE.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.
	OE.INSTALL	OE.INSTALL ensures that the TOE will be installed correctly and configured securely.
A.EXTERNAL The external syslog server and any external authentication servers are operating correctly and securely. Data transmitted between the TOE and the external servers is protected from tampering by untrusted subjects both during transfer to the external server, during storage on the external server, and during transmission to the TOE from the external server.	OE.EXTERNAL	OE.EXTERNAL ensures that that authentication data will be kept secure outside of the TOE boundary.
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.	OE.CREDENTIALS	OE.CREDENTIALS ensures that users and Administrators will set secure passwords, making it harder for an unauthorized person gain access to the TOE.
A.DISCLOSE Users and administrators will not disclose their passwords.	OE.CREDENTIALS	OE.CREDENTIALS ensures that users and Administrators will not share their passwords, making it harder for an unauthorized person gain access to the TOE.

8.2 Security Functional Requirements Rationale

The following discussion provides detailed evidence of coverage for each security objective. Table 16 demonstrates the mapping from the security objectives to the SFRs is complete. The following discussion provides detailed evidence of coverage for each objective.

Table 16 - Mapping of Security Objectives to Security Functional Requirements

Objectives / SFRs	O.AUDIT	O.INTACC	O.ADMIN	O.TIME	O.AUTHENTICATE	O.PROTECT
FAU_GEN.1	✓					
FAU_SAR.1	✓					
FAU_SAR.3	✓					
FAU_STG.1	✓					
FDP_ACC.1a			✓			
FDP_ACC.1b		✓				
FDP_ACF.1a			✓			
FDP_ACF.1b		✓				
FDP_IFC.1		✓				
FDP_IFF.1		✓				
FIA_UAU.2		✓			✓	
FIA_UID.2		✓			✓	
FMT_MOF.1			✓			
FMT_MSA.1			✓			
FMT_MSA.3a			✓			
FMT_MSA.3b		✓	✓			
FMT_MSA.3c		✓	✓			
FMT_MTD.1			✓			
FMT_SMF.1			✓			

Objectives / SFRs	O.AUDIT	O.INTACC	O.ADMIN	O.TIME	O.AUTHENTICATE	O.PROTECT
FMT_SMR.1			✓			
FPT_RVM.1						✓
FPT_SEP.1						✓
FPT_STM.1				✓		

8.2.1 Rationale for Security Functional Requirements of the TOE Objectives

Table 17 - Objectives: SFRs Mapping

Objective	Requirements Addressing the Objective	Rationale
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_GEN.1	FAU_GEN.1 requires that the TOE record all commands entered by an Administrator (except actions performed at the underlying FreeBSD shell).
	FAU_SAR.1	FAU_SAR.1 requires that the TOE provide the authorized administrators with the ability to read the audit records.
	FAU_SAR.3	FAU_SAR.3 requires that the TOE provide the authorized administrators with the ability to search the audit records.
	FAU_STG.1	FAU_STG.1 requires that the TOE protect the audit records it holds.
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_ACC.1b	FDP_ACC.1b requires the TOE to enforce the VPN User Access Control SFP.
	FDP_ACF.1b	FDP_ACF.1b specifies the attributes used to enforce the VPN User Access Control SFP.
	FDP_IFC.1	FDP_IFC.1 requires the TOE to enforce the VPN Information Flow Control SFP.
	FDP_IFF.1	FDP_IFF.1 specifies the attributes used to enforce the VPN Information Flow Control SFP.
	FIA_UAU.2	FIA_UAU.2 requires VPN users to be authenticated before they are able to perform any other actions.

Objective	Requirements Addressing the Objective	Rationale
	FIA_UID.2	FIA_UID.2 requires VPN users to be identified before they are able to perform any other actions.
	FMT_MSA.3b	FMT_MSA.3b defines static attribute initialization for the VPN User Access Control SFP and who can modify the default values.
	FMT_MSA.3c	FMT_MSA.3c defines static attribute initialization for the VPN User Information Flow Control SFP and who can modify the default values.
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.	FDP_ACC.1a	FDP_ACC.1a requires the TOE to enforce the Administrator Access Control SFP.
	FDP_ACF.1a	FDP_ACF.1a specifies the attributes used to enforce the Administrator Access Control SFP.
	FMT_MOF.1	FMT_MOF.1 restricts access to TOE management functions.
	FMT_MSA.1	FMT_MSA.1 specifies which roles can access security attributes.
	FMT_MSA.3a	FMT_MSA.3a defines static attribute initialization for the Administrator Access Control SFP and who can modify the default values.
	FMT_MSA.3b	FMT_MSA.3b defines static attribute initialization for the VPN User Access Control SFP and who can modify the default values.
	FMT_MSA.3c	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	FMT_MTD.1 specifies which roles can access TSF data.
	FMT_SMF.1	FMT_SMF.1 specifies the management functions the TOE must provide.
	FMT_SMR.1	FMT_SMR.1 requires the TOE to maintain separate Administrator roles.
O.TIME The TOE must provide reliable timestamps for its own use.	FPT_STM.1	FPT_STM.1 requires that the TOE provide reliable timestamps for its own use.
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	FIA_UAU.2 requires Administrators to be authenticated before they are able to perform any other actions.
	FIA_UID.2	FIA_UID.2 requires Administrators to be identified before they are able to perform any other actions.
O.PROTECT	FPT_RVM.1	FPT_RVM.1 requires that the security functions are non-

Objective	Requirements Addressing the Objective	Rationale
The TOE must ensure the integrity of audit and system data by protecting itself from unauthorized modifications and access to its functions and data.		bypassable.
	FPT_SEP.1	FPT_SEP.1 requires that the TOE protect itself from interference and tampering by untrusted subjects.

8.2.2 Rationale for Security Functional Requirements of the IT Environment

Table 18 - Environmental Objectives: Environmental SFRs Mapping

Objective	Requirements Addressing the Objective	Rationale
N/A	N/A	N/A

8.3 Security Assurance Requirements Rationale

EAL2 augmented with ALC_FLR.1 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.1, the System will have incurred a search for obvious flaws to support its introduction into the non-hostile environment.

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

8.4 Rationale for Explicitly-defined Security Functional Requirements

There are no explicitly-defined Security Functional Requirements.

8.5 Rationale for Refinements of Security Functional Requirements

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

- FMT_MOF.1
- The words "**as specified in Table 8 above**" were added to FMT_MOF.1.1 so that all of the access control requirements could be consolidated into a single table for clarification of the administrator roles.

8.6 Dependency Rationale

This ST does satisfy all the requirement dependencies of the Common Criteria. Table 19 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 19 - Functional Requirements Dependencies

SFR	Dependencies	Dependency Met	Rationale
FAU_GEN.1	FPT_STM.1	✓	
FAU_SAR.1	FAU_GEN.1	✓	
FAU_SAR.3	FAU_SAR.1	✓	
FAU_STG.1	FAU_GEN.1	✓	
FDP_ACC.1	FDP_ACF.1	✓	
FDP_ACF.1	FDP_ACC.1	✓	
	FMT_MSA.3	✓	
FDP_IFC.1	FDP_IFF.1	✓	
FDP_IFF.1	FDP_IFC.1	✓	
	FMT_MSA.3	✓	
FIA_UAU.2	FIA_UID.1		Although FIA_UID.1 is not included, FIA_UID.2, which is hierarchical to FIA_UID.1, is included. This satisfies this dependency.
FIA_UID.2	No dependencies	✓	
FMT_MOF.1	FMT_SMF.1	✓	
	FMT_SMR.1	✓	
FMT_MSA.1	FDP_ACC.1 or FDP_IFC.1	✓	FDP_ACC.1 is included.
	FMT_SMR.1	✓	
	FMT_SMF.1	✓	

SFR	Dependencies	Dependency Met	Rationale
FMT_MSA.3	FMT_MSA.1	✓	
	FMT_SMR.1	✓	
FMT_MTD.1	FMT_SMF.1	✓	
	FMT_SMR.1	✓	
FMT_SMF.1	No dependencies	✓	
FMT_SMR.1	FIA_UID.1		Although FIA_UID.1 is not included, FIA_UID.2, which is hierarchical to FIA_UID.1, is included. This satisfies this dependency.
FPT_RVM.1	No dependencies	✓	
FPT_SEP.1	No dependencies	✓	
FPT_STM.1	No dependencies	✓	

8.7 TOE Summary Specification Rationale

8.7.1 TOE Summary Specification Rationale for the Security Functional Requirements

Each subsection in the TOE Summary Specification (Section 6) describes a security function of the TOE. Each description is organized by set of requirements with rationale that indicates how these requirements are satisfied by aspects of the corresponding security function. The set of security functions works to satisfy all of the security functions and assurance requirements. Furthermore, all of the security functions are necessary in order for the TSF to provide the required security functionality. This section, in conjunction with the TOE Summary Specification section, provides evidence that the security functions are suitable to fulfill the TOE security requirements.

Table 11 identifies the relationship between security requirements and security functions, showing that all security requirements are addressed and all security functions are necessary (i.e., they correspond to at least one security requirement).

The only security mechanism that is realized by a probabilistic or permutational implementation is the password mechanism of the Identification and Authentication Security Function. A strength of function rating of *SOF-basic* is claimed for the TOE’s Security Functions. For an analysis of the Strength of Function, refer to Section 8.8 below.

8.8 Strength of Function

Strength of function rating of *SOF-basic* is claimed for this TOE to meet the EAL2 augmented with ALC_FLR.1 assurance requirements, this SOF is sufficient to resist the threats identified in Section 3.2. Section 8.1 provides evidence that demonstrates that TOE threats are countered by the TOE security objectives. Section 8.2 demonstrates that the security objectives for the TOE and the TOE environment are satisfied by the security requirements. The evaluated TOE is intended to operate in commercial and Department of Defense low robustness environments processing unclassified information.

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

The relevant security function and security functional requirements which have probabilistic or permutational functions are Identification and Authentication (FIA_UID.2 and FIA_UAU.2).

9 Acronyms

Table 20 - Acronyms

Acronym	Definition
CC	Common Criteria for Information Technology Security Evaluation
CLI	Command Line Interface
EAL	Evaluation Assurance Level
IP	Internet Protocol
ISO	International Organization for Standardization
IT	Information Technology
LCD	Liquid Crystal Display
LDAP	Lightweight Directory Access Protocol
PP	Protection Profile
RADIUS	Remote Authentication Dial In User Service
SAR	Security Assurance Requirement
SFR	Security Functional Requirement
SOF	Strength of Function
SSL	Secure Sockets Layer
ST	Security Target
TACACS+	Terminal Access Controller Access-Control System Plus
TCP	Transmission Control Protocol
TOE	Target of Evaluation
TSC	TOE Scope of Control
TSF	TOE Security Function

Acronym	Definition
TSP	TOE Security Policy
VPN	Virtual Private Network