Common Criteria Security Target

For

NetScaler Platinum Edition Load Balancer Version 9.2

Version 1-1 3 August 2011

Summary of Amendments

Version 1-1 3 August 2011

Updated to remove erroneous mentions of ‘NetScaler Configuration Utility’ in section 6.

Version 1-0 28 January 2011

First released version.

0. Preface

0.1 Objectives of Document

This document presents the Common Criteria (CC) Security Target (ST) to express the security and evaluation requirements for the Citrix NetScaler Platinum Edition Load Balancer Version 9.2 product.

The product is designed and manufactured by Citrix Systems Inc. (http://www.citrix.com/).

The Sponsor and Developer for the EAL2 (augmented with ALC_FLR.2) evaluation is Citrix Systems Inc.

0.2 Scope of Document

The scope of the Security Target within the development and evaluation process is described in the Common Criteria for Information Technology Security Evaluation [CC]. In particular, a Security Target defines the IT security requirements of an identified TOE and specifies the functional and assurance security measures offered by that TOE to meet stated requirements [CC1, Section C.1].

Security Functional Requirements (SFRs), as defined in [CC2], are the basis for the TOE IT security functional requirements expressed in this Security Target. These requirements describe the desired security behaviour expected of a TOE and are intended to meet the security objectives as stated in this Security Target. Security Functional Requirements express security requirements intended to counter threats in the assumed operating environment of the TOE, and cover any identified organisational security policies and assumptions.

0.3 Intended Readership

The target audience of this ST are consumers, developers, evaluators and certifiers of the TOE, additional information can be found in [CC1, Section 6.2].

0.4 Related Documents

Common Criteria[1]

[1] For details see http://www.commoncriteriaportal.org/

[CC1] Common Criteria for Information Technology Security Evaluation,
Part 1: Introduction and General Model,
CCMB-2009-07-001, Version 3.1 Revision 3, July 2009.

[CC2] Common Criteria for Information Technology Security Evaluation,
Part 2: Security Functional Components,
CCMB-2009-07-002, Version 3.1 Revision 3, July 2009.

[CC3] Common Criteria for Information Technology Security Evaluation,
Part 3: Security Assurance Components,
CCMB-2009-07-003, Version 3.1 Revision 3, July 2009.

[CEM] Common Methodology for Information Technology Security Evaluation,
Evaluation Methodology,
CCMB-2009-07-004, Version 3.1, Revision 3, July 2009.

Other documentation

[CCECG] Common Criteria Evaluated Configuration Guide for NetScaler 9.2 Platinum Edition, Document code: Jan 22 2011 04:11:22

[FIPS140] CMVP FIPS 140-2 certificate #1369: Nitrox XL 1600-NFBE HSM Family

[VPX-GS] Citrix NetScaler VPX Getting Started Guide – Citrix NetScaler VPX 9.2.e, Document code: December 20 2010 07:06:30

[XS ST] Common Criteria Security Target for Citrix XenServer 5.6 Platinum Edition, v1-0, 30 July 2010

0.5 Significant Assumptions

None.

0.6 Outstanding Issues

None.

0.7 Glossary

Term	Meaning
Assurance	Grounds for confidence that a TOE meets the SFRs [CC1].
CC	Common Criteria
CLI	Command Line Interface

Term	Meaning
CM	Configuration Management
DNS	Domain Name System
dom0	See Domain 0.
domU	See Domain U.
Domain	A running instance of a virtual machine. (In a XenServer environment a virtual machine can exist even when not running, however in this Security Target the terms 'domain' and 'virtual machine' are equivalent.)
Domain 0	A special-purpose domain that exists in a single instance on each XenServer host. Domain 0 is the only privileged domain (meaning that it can use privileged hypervisor calls) on a XenServer host, and is thus the only domain that can control access to physical input/output resources directly and access the content of other domains (i.e. Domain U).
Domain U	The collection of XenServer domains other than Domain 0. In the case of the NetScaler TOE, Domain U consists of a single HVM Guest.
Domain U Guest	An unprivileged domain maintained by XenServer. In the case of the NetScaler TOE, Domain U consists of a single HVM Guest.
EAL	Evaluation Assurance Level
FIPS	Federal Information Processing Standard
FTP	File Transfer Protocol
GUI	Graphical User Interface
Host	An installation of XenServer on a dedicated server.
HTTP	Hypertext Transfer Protocol
HTTPS	Secure Hypertext Transfer Protocol
HVM Guest	A XenServer domain (in domU) running a VM with an OS that is not aware that it is in a virtualised environment.
Hypercall	Synchronous calls made from a domain to the hypervisor. Any domain may make calls to the hypervisor, but only dom0 can make privileged calls, such as those that cause memory (including memory representing physical resources) to be mapped into or out of domains.
Hypervisor	An abstraction layer implementing a set of software calls (hypercalls) that can be made by XenServer domains, and controlling the underlying hardware on a XenServer host (e.g. scheduling of the CPU and partitioning of memory between virtual machines).

Term	Meaning
HVM Guest	A member of domU in which an unmodified Guest OS can be installed and run. This is contrasted with a PV Guest, in which the Guest OS is modified to be aware of its virtualised environment. The VPX platform of the TOE runs in an HVM Guest domain, with PV drivers installed.
IP	Internet Protocol
LCD	Liquid Crystal Display
LDAP	Lightweight Directory Access Protocol
NNTP	Network News Transfer Protocol
Pool	A group of XenServer hosts in which one host takes the role of master and the others are slaves. Storage and configuration metadata are shared across the pool.
PP	Protection Profile
PV Drivers	Drivers that replace default drivers in an HVM Guest, in order to accelerate storage and network data paths. These are treated as part of the Guest OS, use unprivileged XenServer interfaces, and are not involved in implementing XenServer security functions.
RADIUS	Remote Authentication Dial-In User Service
SAR	Security Assurance Requirement
SCP	Secure Copy
SFP	Security Function Policy
SFR	Security Functional Requirement
SFTP	Secure Shell File Transfer Protocol
SSH	Secure Shell
SSL	Secure Sockets Layer
ST	Security Target
Target of Evaluation	A set of software, firmware and/or hardware possibly accompanied by guidance. [CC1]
TCP	Transmission Control Protocol
TOE	Target of Evaluation
TOE Security Functionality	A set consisting of all hardware, software, and firmware of the TOE that must be relied upon for the correct enforcement of the SFRs. [CC1]
TSF	TOE Security Functionality
URL	Uniform Resource Locator
VM	Virtual Machine

Term	Meaning
Virtual Machine	An abstraction of a real hardware machine that creates an environment in which software (typically an operating system) that would otherwise run directly on hardware as the only software to be executing can be run with the illusion of exclusive access to a set of physical resources. In XenServer a virtual machine is characterised by a defined set of resources (e.g. memory and storage capacities and available network connections). A virtual machine that has been allocated real resources and in which processes are running is a Domain.
VPN	Virtual Private Network
WAN	Wide Area Network

See [CC1] for other Common Criteria abbreviations and terminology.

Contents

1. ST Introduction 10
   1.1 ST and TOE Reference Identification 10
   1.2 TOE Description 10
      1.2.1 NetScaler Product Overview 10
      1.2.2 Load Balancer 11
         1.2.2.1 Load Balancing Virtual Servers 12
         1.2.2.2 Content Switching 12
         1.2.2.3 SSL Acceleration 12
         1.2.2.4 AppCache 12
         1.2.2.5 AppCompress 13
         1.2.2.6 Surge Protection 13
      1.2.3 Access Gateway 13
      1.2.4 Web Application Firewall 13
      1.2.5 Application Delivery Networking Platform 13
      1.2.6 MPX Hardware Appliances 13
      1.2.7 VPX Virtualised Platform 14
   1.3 TOE Overview 14
      1.3.1 Components of the TOE 15
      1.3.2 Guidance Documentation 16
      1.3.3 Required non-TOE hardware and software 16
      1.3.4 TOE Environment 17
   1.4 TOE Description 18
      1.4.1 Physical Scope 18
      1.4.2 Logical Scope 18
         1.4.2.1 Security Audit 20
         1.4.2.2 User Data Protection 20
         1.4.2.3 Identification and Authentication 20
         1.4.2.4 Security Management 20
         1.4.2.5 Protection of the TSF 20
      1.4.3 Product Physical/Logical Features and Functionality not included in the TOE 20
2. CC Conformance 22
3. Security Problem Definition 23
   3.1 Threats 23
      3.1.1 T.AccessInt Unauthorised access to internal network 23
      3.1.2 T.AccessTOE Unauthorised access to TOE data 23
      3.1.3 T.Unavail Unavailability of TOE services 23
      3.1.4 T.Masquerade Masquerade as another entity 23
      3.1.5 T.ModConf Unauthorised modification of configuration 24
      3.1.6 T.Bypass 24
   3.2 Organisational Security Policies 24
   3.3 Assumptions 24
      3.3.1 A.Crypto Protection of cryptographic data 24
      3.3.2 A.AuthData Protection of authentication data 24
      3.3.3 A.External Protected external authentication servers 24
      3.3.4 A.Install Secure installation 24
      3.3.5 A.Locate Physically secure TOE location 25
      3.3.6 A.Manage Administrator security responsibility 25
      3.3.7 A.NetCon Secure network administration 25
4. Security Objectives 26
   4.1 Security Objectives for the TOE 26
      4.1.1 O.Admin Controlled administrator operations 26
      4.1.2 O.Audit Audit of administrator actions 26
      4.1.3 O.Authenticate Adminstrator authentication 26

4.1.4 O.IntAcc Internal network access control 26
4.1.5 O.ExtAcc External network access control 26
4.1.6 O.Time Reliable timestamps 26
4.2 Security Objectives for the Operational Environment 26
4.2.1 OE.Connect Network connection 27
4.2.2 OE.External Protected external authentication data 27
4.2.3 OE.Crypto Protected cryptographic data 27
4.2.4 OE.Credentials Secure passwords 27
4.2.5 OE.Install Correct installation 27
4.2.6 OE.Manage Administrator checks 27
4.2.7 OE.Physical Secure physical environment 27
4.3 Security Objectives Rationale 27
5. IT Security Requirements 32
5.1 Conventions 32
5.2 Security Functional Requirements 32
5.2.1 Administrator Authentication 32
5.2.2 Administrator command access 33
5.2.3 VPN connection access 34
5.2.4 Internal network resource access 35
5.2.5 Network traffic access 36
5.2.6 Security Management 38
5.2.7 Audit and Timestamping 42
5.3 Security Assurance Requirements 44
5.4 Security Requirements Rationale 46
5.4.1 Mapping between SFRs and Security Objectives 46
5.4.2 SFR Dependencies Analysis 48
6. TOE Summary Specification 51
6.1 Security Audit 51
6.2 User Data Protection 51
6.2.1 Administrator Access Control SFP 51
6.2.2 VPN Access Control SFP 52
6.2.3 VPN Information Flow Control SFP 52
6.2.4 Web Application Firewall Information Flow Control SFP 53
6.3 Identification and Authentication 53
6.4 Security Management 53
6.5 Timestamps 54

Figures / Tables

Figure 1: Deployment Configuration of the Product 11
Figure 2: TOE Boundary 15
Figure 3: VPX Platform TOE detail 19
Table 1: Threats/ Assumptions addressed by Security Objectives 28
Table 2: Security Management Matrix 40
Table 3: Security Assurance Requirements 44
Table 4: Objectives implemented by SFRs 46
Table 5: Analysis of SFR dependencies 50

1. ST Introduction

1.1 ST and TOE Reference Identification

TOE Reference:	NetScaler Platinum Edition Load Balancer Version 9.2
ST Reference:	CIN6-ST-0001
ST Version:	1-1
ST Date:	3 August 2011
Assurance Level:	EAL2 augmented with ALC_FLR.2 Flaw Reporting Procedures
ST Author:	SiVenture

1.2 TOE Description

1.2.1 NetScaler Product Overview

The TOE is the Citrix NetScaler Platinum Edition Load Balancer Version 9.2, with software build 48.600102.e.nc (abbreviated in this document to "NetScaler"). NetScaler is an application performance accelerator incorporating a Secure Sockets Layer (SSL) Virtual Private Network (VPN) with policy-based access control and a Web Application Firewall. The scope of this evaluation includes the TOE when operating as a dedicated self-contained appliance (i.e. running on dedicated hardware supplied as part of the TOE) and when running on the Citrix XenServer hardware virtualisation product (installed on conventional server hardware containing CPU support for virtualisation). Figure 1 below shows the details of the deployment configuration of the TOE:

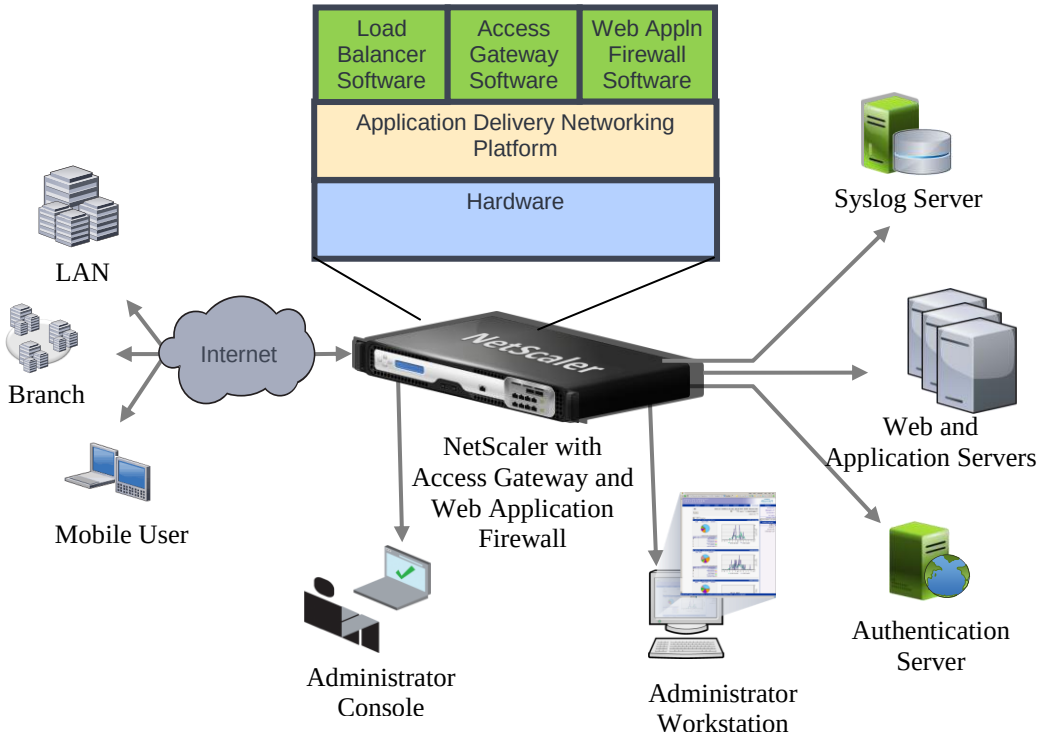

Figure 1: Deployment Configuration of the Product

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 either a dedicated MPX hardware appliance (the specific appliances within the scope of this Security Target are listed in section 1.3.1) or within a virtual machine managed by XenServer running on generic server 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 (SSH).

1.2.2 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.

1.2.2.1 Load Balancing Virtual Servers

The Load Balancer allows the definition of Load Balancing virtual servers (vserver). Each Load Balancing vserver consists of an IP 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, FTP, HTTPS, NNTP, and DNS.

1.2.2.2 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.

1.2.2.3 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.

1.2.2.4 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.

1.2.2.5 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[2], which yields up to 50% reduction in bandwidth requirements and improves end-user performance.

1.2.2.6 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.

1.2.3 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.

1.2.4 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.

1.2.5 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 assure that critical applications receive the highest priority and are not pre-empted by lower-priority operations.

1.2.6 MPX Hardware Appliances

The TOE hardware appliances consist of the following platforms: MPX 5500, MPX 9700-FIPS, MPX 10500-FIPS, MPX 12500-FIPS, MPX 15500-FIPS, MPX 7500, MPX 9500, MPX 10500, MPX 12500, MPX 15500, MPX 17500, and MPX 19500. These units support

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

Fast Ethernet and/or copper Gigabit Ethernet depending on the models. 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 "FIPS Series" models [FIPS].

1.2.7 VPX Virtualised Platform

The TOE can also be run in a virtual machine under XenServer on generic server hardware[3]. In this case XenServer and the server hardware are not part of the TOE. The TOE has 4 different configurations on the virtualised platform: VPX-10, VPX-200, VPX-1000, and VPX-3000. The configuration is determined by the license in use, and distinguished by the maximum throughput available.

1.3 TOE Overview

The TOE Overview summarizes the usage and major security features of the TOE. It 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:

[3] The hardware is subject to certain minimum requirements as described in [VPX-GS], and uses XenServer in its evaluated configuration as described in [XS ST], except that the domU HVM guest VM used is the one supplied with NetScaler instead of a Windows VM.

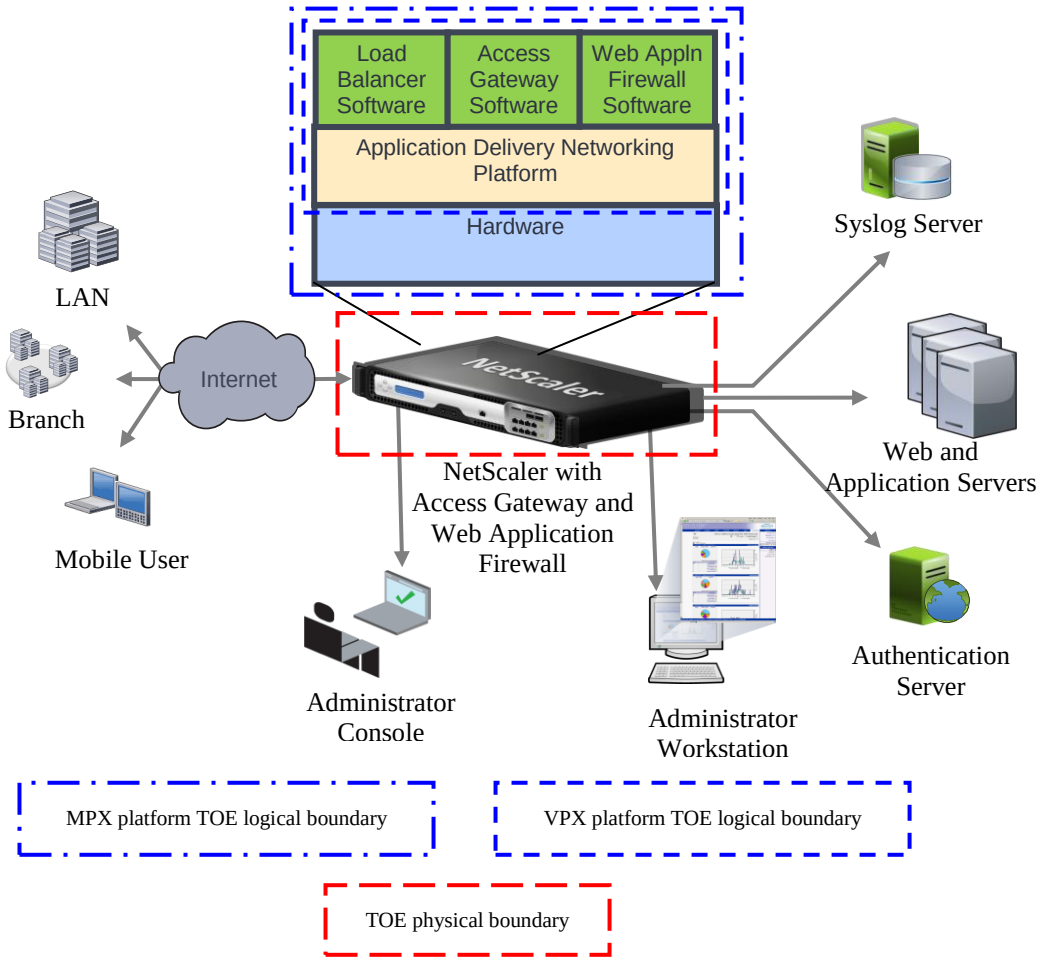

Figure 2: TOE Boundary

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.

1.3.1 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. When deployed on an MPX platform, the TOE includes the hardware appliance (see list of platforms below); when running on a VPX platform, the server hardware and XenServer virtualisation software are part of the TOE environment.

The hardware appliances in the scope of this ST are:

- MPX 5500 Platform
- MPX 9700-FIPS Platform

- MPX 10500-FIPS Platform
- MPX 12500-FIPS Platform
- MPX 15500-FIPS Platform
- MPX 7500 Platform
- MPX 9500 Platform
- MPX 10500 Platform
- MPX 12500 Platform
- MPX 15500 Platform
- MPX 17500 Platform
- MPX 19500 Platform.

The virtualised platforms (all running XenServer 5.6 (on PC hardware meeting the minimum specification in [VPX-GS]) are:

- VPX-10
- VPX-200
- VPX-1000
- VPX-3000.

In the remainder of this document, use of the TOE on its own hardware appliances is referred to as deployment on the 'MPX platforms'; use of the TOE in the virtualised environment is referred to as deployment on the 'VPX platform'.

1.3.2 Guidance Documentation

The following guide is required reading and forms part of the TOE:

- Common Criteria Evaluated Configuration Guide for NetScaler 9.2 Platinum Edition, Document code: Jan 22 2011 04:11:22 [CCECG]

1.3.3 Required non-TOE hardware and software

When deployed on the MPX platforms, no additional non-TOE hardware or software is required.

When deployed on the VPX platform, the following non-TOE hardware or software is required:

- XenServer 5.6
- Server hardware meeting requirements specified for the VPX platform in [VPX-GS]

- XenCenter.

1.3.4 TOE Environment

The TOE environment consists of the following hardware and software:

- Administrator console and workstation for management of the TOE
    - XenCenter is used for installation of the NetScaler software on the VPX platform in [CCECG], but is not required for normal operation of the TOE. It is also possible to install the NetScaler software using the XenAPI without the use of XenCenter.
    - The NetScaler VPX console application is used for initial configuration of NetScaler on the VPX platform. Routine management of NetScaler after installation on the VPX platform can be carried out using either the VPX console application or the NetScaler command line interface used for MPX platforms.
- Application server(s)
- Syslog server (optional)
- VPN client(s)
- Networks (including the Internet and the Corporate Office Network)
- Authentication server (RADIUS, LDAP) (optional).

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 travelling 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 implement this configuration.

The TOE is managed through a CLI[4] (and the CLI therefore forms part of the TOE) Administrators must access this interfaces from a trusted workstation that supports SSH or from a workstation on a direct serial connection.

1.4 TOE Description

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

The TOE is an application performance accelerator[5] running on the MPX and VPX platforms listed in section 1.3.1.

1.4.1 Physical Scope

Figure 2 shows the physical scope and the physical boundary of the TOE within the context of a deployment of the NetScaler product. In the MPX case the physical boundary is defined by the appliance itself. In the VPX case the physical boundary is defined by the physical boundary of the XenServer host on which NetScaler is installed.

The different hardware configurations for the MPX platform are listed in section 1.3.1.

1.4.2 Logical Scope

The logical boundary of the TOE is shown in Figure 2 above.

There are several logical components of the TOE: the 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 Functionality (TSF). The logical components run directly on the NetScaler appliance hardware in the case of the MPX platforms, and in a virtual machine in the case of the VPX platform. A more detailed view of the TOE in the VPX case is shown in Figure 3.

[4] Note that management via the GUI Dashboard Command Centre (or by clients using the NetScaler XML-API) is not included in the scope of the TOE. The evaluated configuration disables the use of these features as described in [CCECG].

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

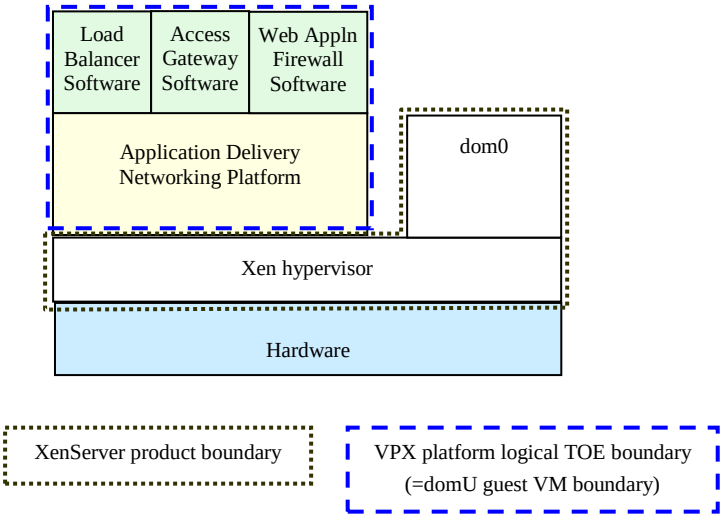

Figure 3: VPX Platform TOE detail

The VPX platform TOE runs in a virtual machine (VM) under XenServer (in XenServer terminology NetScaler runs in an HVM Guest domain, or 'domU guest', with PV drivers installed). The Application Delivery Network Platform in this case provides not only the supporting functions for the Load Balancer, Access Gateway and Application Firewall software, but also the VM operating system[6]. The Xen hypervisor and dom0 are parts of the XenServer environment for the VPX platform, and together provide the mapping of virtual resources in the domU guest VM to the physical resources on the host hardware (there is no equivalent of the hypervisor or dom0 in the MPX case where the logical components run directly on the appliance hardware).

On the VPX platform the XenServer host is not a member of a XenServer Pool[7], and runs only two domains: dom0 and the NetScaler domU guest.

The TOE's logical boundary includes all of the TSF. 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

[6] On the VPX platform the Application Delivery Networking Platform therefore acts as the operating system that manages the resources provided by the virtual machine, in the same way as on the MPX platform it acts as the operating system that manages the resources provided by the appliance hardware.

[7] The evaluated configuration of XenServer in [XS ST] allows XenServer hosts to be linked together to create a 'pool'. In the case of a NetScaler VPX platform, the XenServer host is the only member of its 'pool'.

- FMT Security Management
- FPT Protection of the TSF.

These functions are discussed in detail below.

1.4.2.1 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.

1.4.2.2 User Data Protection

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

1.4.2.3 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 and digital certificates.

1.4.2.4 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.

1.4.2.5 Protection of the TSF

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

1.4.3 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
- NetScaler GUI Dashboard Command Center application and NetScaler XML-API interface[8].

In addition, any other features or functionality not mentioned explicitly as part of the TOE in Sections 1.3 and 1.4 are excluded from the TOE.

[8] These are altenative methods of managing NetScaler. However, only the CLI method of management is included in the evaluated configuration.

2. CC Conformance

As defined by the references [CC1], [CC2] and [CC3], this TOE conforms to the requirements of Common Criteria v3.1, Revision 3. The methodology applied for the evaluation is defined in [CEM].

The TOE is Part 2 conformant, Part 3 conformant, and meets the requirements of EAL2 augmented with ALC_FLR.2 Flaw Reporting Procedures.

This ST does not claim conformance to any PP.

3. Security Problem Definition

3.1 Threats

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 be capable of attacks at Basic attack potential (as covered by the AVA_VAN.2 assurance component). 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 to be countered by the TOE and its environment.

3.1.1 T.AccessInt Unauthorised access to internal network

A user might gain unauthorised access to internal network resources.

3.1.2 T.AccessTOE Unauthorised access to TOE data

A user may gain unauthorized access to security data on the TOE.

3.1.3 T.Unavail Unavailability of TOE services

An authorized user may not be able to utilise NetScaler services due to physical tampering of the TOE or the network.

3.1.4 T.Masquerade Masquerade as another entity

A user or process may attempt to obtain credentials for another entity in order to gain unauthorized access to data or TOE resources.

3.1.5 T.ModConf Unauthorised modification of configuration

An attacker or unauthorized user may modify a user's configuration. This covers: modification of the user's set of permitted internal network resources and modification of configuration data associated with a user.

3.1.6 T.Bypass

A user or process may be able to bypass the TOE's security mechanisms thereby compromising TOE user or system data.

3.2 Organisational Security Policies

No organisational security policies are defined for the TOE.

3.3 Assumptions

The following assumptions are made regarding the TOE:

3.3.1 A.Crypto Protection of cryptographic data

The TOE environment will ensure that the TOE stored cryptographic data is protected against tampering.

3.3.2 A.AuthData Protection of authentication data

Users and administrators will choose sufficiently strong passwords (relative to the risk in the deployment environment, and any password policies in force), and maintain their confidentiality.

3.3.3 A.External Protected external authentication servers

The external authentication servers are operating correctly and securely (relative to the risk in the deployment environment, and any relevant policies in force). Data transmitted between the TOE and the external servers is protected from tampering by untrusted subjects during transfer to the external server, during storage on the external server, and during transmission to the TOE from the external server.

3.3.4 A.Install Secure installation

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.

3.3.5 A.Locate Physically secure TOE location

The TOE is located within a controlled access facility which restricts physical access to the appliance to authorized persons only. The location must provide uninterruptible power (protected against surges), air conditioning, and all other conditions required for reliable operation of the hardware.

3.3.6 A.Manage Administrator security responsibility

One or more competent individuals are assigned the role of administrator to manage the TOE and the security of the information it contains.

3.3.7 A.NetCon Secure network administration

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.

4. Security Objectives

4.1 Security Objectives for the TOE

The security objectives for NetScaler are defined as follows.

4.1.1 O.Admin Controlled administrator operations

The TOE must include a set of operations 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.

4.1.2 O.Audit Audit of administrator actions

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.

4.1.3 O.Authenticate Adminstrator authentication

The TOE must be able to identify and authenticate administrators prior to allowing access to TOE administrative functions and data.

4.1.4 O.IntAcc Internal network access control

The TOE must allow access to internal network resources only as defined by the VPN Access Control SFP and the VPN Information Flow Control SFP.

4.1.5 O.ExtAcc External network access control

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.

4.1.6 O.Time Reliable timestamps

The TOE must provide reliable timestamps for its own use.

4.2 Security Objectives for the Operational Environment

The objectives that are required to be met by the TOE's operational environment are as follows.

4.2.1 OE.Connect Network connection

The TOE environment must provide network connectivity to the TOE. The network connection to the TOE must be reliable.

4.2.2 OE.External Protected external authentication data

The TOE environment must ensure any authentication data in the environment are protected and correctly maintained.

4.2.3 OE.Crypto Protected cryptographic data

The TOE environment must ensure that the stored cryptographic data is protected against tampering.

4.2.4 OE.Credentials Secure passwords

Users and administrators will set sufficiently strong passwords (relative to the risk in the deployment environment, and any password policies in force), and maintain their confidentiality.

4.2.5 OE.Install Correct installation

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.

4.2.6 OE.Manage Administrator checks

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.

4.2.7 OE.Physical Secure physical environment

The physical environment must provide the TOE with a secure setting, and with uninterruptible power (protected against surges), air conditioning, and all other conditions required for reliable operation of the hardware.

4.3 Security Objectives Rationale

The ways in which the threats are addressed by the security objectives are summarised in Table 1.

Threat/ OSP/ Assumption / Security Objectives	T. AccessInt	T.AccessTOE	T.Unavail	T.Masquerade	T.ModConf	T.Bypass	A.Crypto	A.AuthData	A.External	A.Install	A.Locate	A.Manage	A.NetCon
O.Admin		X											
O.Audit		X		X	X								
O.Authenticate		X		X	X								
O.IntAcc	X												
O.ExtAcc	X												
O.Time	X	X											
OE.Connect			X			X					X		X
OE.External		X			X				X		X		X
OE.Crypto							X						
OE.Credentials	X	X		X				X					
OE.Install	X	X								X		X	
OE.Manage	X	X			X					X		X	
OE.Physical			X			X					X		

Table 1: Threats/ Assumptions addressed by Security Objectives

T.AccessInt is addressed by objectives as follows:

- O.IntAcc ensures that the TOE limits access to internal network resources to the authorized users
- O.ExtAcc ensures that the TOE limits communications between itself and external IT entities based on the Web Application Firewall rules
- O.Time ensures that the TOE maintains the correct time to be used when the date and time are determining factors for access
- OE.Credentials ensures that users will not share their passwords, making it harder for an unauthorized person gain access to the TOE
- 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.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.

T.AccessTOE is addressed by objectives as follows:

- O.Admin ensures that only Administrators can access the management functions for the TOE
- 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.Authenticate ensures that Administrators identify and authenticate themselves before they are given access
- O.Time ensures that the TOE has the correct time when recording audit records
- OE.External ensures that authentication data is stored securely outside of the TOE
- OE.Credentials ensures that Administrators will not share their passwords, making it harder for an unauthorized person gain access to the TOE
- OE.Install ensures that the TOE will be installed correctly and configured securely
- 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.

T.Unavail is addressed by objectives as follows:

- OE.Connect ensures that the TOE has a reliable network connection
- OE.Physical ensures that the environment will protect the TOE from physical tampering.

T.Masquerade is addressed by objectives as follows:

- O.Authenticate ensures that Administrators supply login credentials before being granted management access to the TOE
- OE.Credentials ensures that Administrators will not share their passwords, making it harder for an unauthorized person to pretend to be an authorized Administrator
- O.Audit ensures that events of security relevance (such as Administrator login) are audited (except actions performed at the underlying FreeBSD shell), hence raising the likelihood that unauthorised access would be noticed and investigated.

T.ModConf is addressed by objectives as follows:

- 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 ensures that Administrators identify and authenticate themselves before they are given access to configuration data

- OE.External ensures that that authentication data is stored securely outside of the TOE

- 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.

T.Bypass is addressed by objectives as follows:

- OE.Connect ensures that the TOE has a network connection

- OE.Physical ensures that the environment will protect the TOE from physical tampering.

A.Crypto is addressed by OE.Crypto, which ensures that the TOE environment will protect the stored cryptographic data against tampering.

A.AuthData is addressed by OE.Credentials, which ensures that users and Administrators will set and maintain secure passwords, making it harder for an unauthorized person gain access to the TOE.

A.External is addressed by OE.External, which ensures that authentication data will be kept secure outside of the TOE boundary.

A.Install is addressed by objectives as follows:

- 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.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.

A.Locate is addressed by objectives as follows:

- OE.Connect ensures that the TOE has a reliable network connection

- OE.External ensures that that authentication data is stored securely outside of the TOE

- OE.Physical ensures that the TOE's environment is suitable for securely supporting the TOE.

A.Manage is addressed by objectives as follows:

- OE.Install ensures that the TOE will be installed correctly and configured securely
- 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.

A.NetCon is addressed by objectives as follows:

- OE.Connect ensures that authentication data is stored securely outside of the TOE
- OE.External ensures that that authentication data will be kept secure outside of the TOE boundary.

5. IT Security Requirements

5.1 Conventions

The following conventions are used for the completion of operations:

- ~~Strikethrough~~ indicates text removed as a refinement and underlined text indicates additional text provided as a refinement.
- [**Bold text within square brackets**] indicates the completion of an assignment.
- [*Italicised text within square brackets*] indicates the completion of a selection.

5.2 Security Functional Requirements

The individual security functional requirements are specified in the sections below.

5.2.1 Administrator Authentication

The only users of the TOE are NetScaler administrative users, who are required to authenticate before being given access to any operations.

FIA_UID.2	**User identification before any action**

Hierarchical to: FIA_UID.1 Timing of identification

Dependencies: No dependencies.

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.

FIA_UAU.2	**User authentication before any action**

Hierarchical to: FIA_UAU.1 Timing of authentication

Dependencies: FIA_UID.1 Timing of identification

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.

Application note:

The users referred to in FIA_UID.2 and FIA_UAU.2 are NetScaler administrators and VPN users.

5.2.2 Administrator command access

FDP_ACC.1/AdminCmd	Subset access control

Hierarchical to: No other components.

Dependencies: FDP_ACF.1 Security attribute based access control

FDP_ACC.1.1/AdminCmd The TSF shall enforce the [**Administrator Access Control SFP**] on [

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

FDP_ACF.1/AdminCmd	Security attribute based access control

Hierarchical to: No other components.

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

FDP_ACF.1.1/AdminCmd 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/AdminCmd 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:**
  - **contains an allow policy for the command and**
  - **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 is a member of a group which is assigned a role that:**
  - **contains a deny policy for the command and**

  - **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:**
  - **assigned a role that contains an allow or deny policy for the command and**
  - **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/AdminCmd 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/AdminCmd 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/AdminCmd**].

5.2.3 VPN connection access

FDP_ACC.1/VPNAccess	**Subset access control**

Hierarchical to: No other components.

Dependencies: FDP_ACF.1 Security attribute based access control

FDP_ACC.1.1/VPNAccess The TSF shall enforce the [**VPN Access Control SFP**] on [

- **Subjects: VPN Clients**
- **Objects: VPN connections**
- **Operations: Establish, Disconnect**].

FDP_ACF.1/VPNAccess	**Security attribute based access control**

Hierarchical to: No other components.

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

FDP_ACF.1.1/VPNAccess 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 address and/or subnet mask**
- **Objects: VPN Connections**
- **Object Attributes: Day and time accessible**].

FDP_ACF.1.2/VPNAccess The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed:

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

FDP_ACF.1.3/VPNAccess The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [**No additional rules**].

FDP_ACF.1.4/VPNAccess The TSF shall explicitly deny access of subjects to objects based on the following additional rules: [**No additional rules**].

5.2.4 Internal network resource access

FDP_IFC.1/IntRes	**Subset information flow control**

Hierarchical to: No other components.

Dependencies: FDP_IFF.1 Simple security attributes

FDP_IFC.1.1/IntRes The TSF shall enforce the [**VPN Information Flow Control SFP**] on

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

FDP_IFF.1/IntRes	**Simple security attributes**

Hierarchical to: No other components.

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

FDP_IFF.1.1/IntRes 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/IntRes 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/IntRes The TSF shall enforce ~~the~~ [**no additional information flow control SFP rules**].

FDP_IFF.1.4/IntRes The TSF shall explicitly authorise an information flow based on the following rules: [**no additional rules**].

FDP_IFF.1.5/IntRes The TSF shall explicitly deny an information flow based on the following rules: [**no additional rules**].

5.2.5 Network traffic access

FDP_IFC.1/Traffic	**Subset information flow control**

Hierarchical to: No other components.

Dependencies: FDP_IFF.1 Simple security attributes

FDP_IFC.1.1/Traffic The TSF shall enforce the [**Web Application Firewall Information Flow Control SFP**] on [

- **Subjects: Internal or external IT entities sending or receiving traffic through the TOE**
- **Information: network traffic flowing through the TOE**
- **Operation: Access**].

FDP_IFF.1/Traffic	**Simple security attributes**

Hierarchical to: No other components.

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

FDP_IFF.1.1/Traffic The TSF shall enforce the [**Web Application Firewall Information Flow Control SFP**] based on the following types of 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/Traffic The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold:

- [**The internal or external IT entity has been granted access to the resource by an administrator based on the subject attributes; and**
- **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/Traffic The TSF shall enforce the [**default condition of denying traffic that has not been authorized by an administrator**].

FDP_IFF.1.4/Traffic The TSF shall explicitly authorise an information flow based on the following rules: [**No additional rules**].

FDP_IFF.1.5/Traffic The TSF shall explicitly deny an information flow between a controlled subject and controlled information via a controlled operation based on the following rules:

- [**The internal or external IT entity has been denied access to the resource by an administrator based on the subject attributes; or**
- **The network traffic information originating from the internal or external IT entity has been denied by an administrator based on the information attributes**].

5.2.6 Security Management

FMT_SMR.1	**Security roles**

Hierarchical to: No other components.

Dependencies: FIA_UID.1 Timing of identification

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.

FMT_SMF.1	**Specification of Management Functions**

Hierarchical to: No other components.

Dependencies: No Dependencies

FMT_SMF.1.1 The TSF shall be capable of performing the following 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**].

FMT_MOF.1	**Management of security functions behaviour**

Hierarchical to: No other components.

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

FMT_MOF.1.1 The TSF shall restrict the ability to [*determine the behaviour of or modify the behaviour of*] the functions [**listed in the Security Management Matrix**[9]] to [**the administrator roles listed in the Security Management Matrix**[9]].

FMT_MSA.1	**Management of security attributes**

Hierarchical to: No other components.

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.1.1 The TSF shall enforce the [**Administrative Access Control SFP**] to restrict the ability to [*query*, *modify*, *delete*, *or* **create as specified in the Security Management Matrix**[9]] the security attributes [**listed in the Security Management Matrix**[9]] to [**the administrative roles outlined in the Security Management Matrix**[9]].

Role	read-only	operator	network	superuser	custom defined role
Security Attributes					
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	query	query, modify	create, delete, query, modify	create, delete, query, modify	As defined

[9] See Table 2.

Role	read-only	operator	network	superuser	custom defined role
permissions					
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
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 permissions			create, delete, query, modify	create, delete, query, modify	As defined

Note regarding Access Control Matrix: "nsroot" (default administrator account) is covered in the table as a special case of the "superuser" account type (unlike other superuser accounts, nsroot cannot be removed). A superuser account provides complete access to all features of the NetScaler and is the only account type 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.

Table 2: Security Management Matrix

FMT_MTD.1	**Management of TSF data**

Hierarchical to: No other components.

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

FMT_MTD.1.1 The TSF shall restrict the ability to [*query*, *modify*, *delete*, **or create as specified in the Security Management Matrix**[9]] the [**TSF data listed in the Security**

Management Matrix[9]] to [**the administrative roles listed in the Security Management Matrix[9]**].

FMT_MSA.3/AdminCmd	**Static attribute initialisation**

Hierarchical to: No other components.

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

FMT_MSA.3.1/AdminCmd 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.3.2/AdminCmd 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.

FMT_MSA.3/VPNAccess	**Static attribute initialisation**

Hierarchical to: No other components.

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

FMT_MSA.3.1/VPNAccess 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/VPNAccess 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.

FMT_MSA.3/IntRes	**Static attribute initialisation**

Hierarchical to: No other components.

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

FMT_MSA3.1/IntRes 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/IntRes 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.

FMT_MSA.3/Traffic	Static attribute initialisation

Hierarchical to: No other components.

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

FMT_MSA.3.1/Traffic 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/Traffic 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.

5.2.7 Audit and Timestamping

FAU_GEN.1	Audit Data Generation

Hierarchical to: No other components.

Dependencies: FPT_STM.1 Reliable time stamps

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*] level of audit;~~ [10] 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**].

[10] There is only one level of audit.

FAU_SAR.1	Audit review

Hierarchical to: No other components.

Dependencies: FAU_GEN.1 Audit data generation

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.

FAU_SAR.3	Selectable audit review

Hierarchical to: No other components.

Dependencies: FAU_SAR.1 Audit review

FAU_SAR.3.1 The TSF shall provide the ability to apply [**searches**] of audit data based on [**keywords through the CLI**].

FAU_STG.1	Protected audit trail storage

Hierarchical to: No other components.

Dependencies: FAU_GEN.1 Audit data generation

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.

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.

FPT_STM.1	Reliable time stamps

Hierarchical to: No other components.

Dependencies: No dependencies

FPT_STM.1.1 The TSF shall be able to provide reliable time stamps.

Application note:

The timestamps support both audit trail entries and, where they are based on time, access control decisions relating to VPN connections (see section 5.2.3).

5.3 Security Assurance Requirements

The security assurance requirements are drawn from [CC3] and represent EAL2, with the addition of ALC_FLR.2 Flaw Reporting Procedures. The assurance components are identified in the table below.

Assurance Class	**Assurance Components**
Security Target (ASE)	ST introduction (ASE_INT.1)
	Conformance claims (ASE_CCL.1)
	Security problem definition (ASE_SPD.1)
	Security objectives (ASE_OBJ.2)
	Extended components definition (ASE_ECD.1)
	Derived security requirements (ASE_REQ.2)
	TOE summary specification (ASE_TSS.1)
Development (ADV)	Security architecture description (ADV_ARC.1)
	Security-enforcing functional specification (ADV_FSP.2)
	Basic design (ADV_TDS.1)
Guidance documents (AGD)	Operational user guidance (AGD_OPE.1)
	Preparative procedures (AGD_PRE.1)
Life cycle support (ALC)	Use of a CM System (ALC_CMC.2)
	Parts of the TOE CM coverage (ALC_CMS.2)
	Delivery procedures (ALC_DEL.1)
	Flaw reporting procedures (ALC_FLR.2)
Tests (ATE)	Evidence of coverage (ATE_COV.1)
	Functional testing (ATE_FUN.1)
	Independent testing – sample (ATE_IND.2)
Vulnerability assessment (AVA)	Vulnerability analysis (AVA_VAN.2)

Table 3: Security Assurance Requirements

The selection of EAL2 is consistent with the assurance levels commonly used for commercial products of this sort, and the augmentation with ALC_FLR.2 provides additional confidence for users that there is a process for reporting and addressing any vulnerabilities that might be

subsequently discovered in the product, and hence that its security will be maintained over time.

5.4 Security Requirements Rationale

5.4.1 Mapping between SFRs and Security Objectives

The mapping between security objectives for the TOE and the SFRs that implement them is summarised in Table 4.

Security Objectives / SFRs	O.Admin	O.Audit	O.Authenticate	O.IntAcc	O.ExtAcc	O.Time
FIA_UID.2			X	X		
FIA_UAU.2			X	X		
FDP_ACC.1/AdminCmd	X					
FDP_ACF.1/AdminCmd	X					
FDP_ACC.1/VPNAccess				X		
FDP_ACF.1/VPNAccess				X		
FDP_IFC.1/IntRes				X		
FDP_IFF.1/IntRes				X		
FDP_IFC.1/Traffic					X	
FDP_IFF.1/Traffic					X	
FMT_SMR.1	X					
FMT_SMF.1	X					
FMT_MOF.1	X					
FMT_MSA.1	X					
FMT_MTD.1	X					
FMT_MSA.3/AdminCmd	X					
FMT_MSA.3/VPNAccess				X		
FMT_MSA.3/IntRes				X		
FMT_MSA.3/Traffic					X	
FAU_GEN.1		X				
FAU_SAR.1		X				
FAU_SAR.3		X				
FAU_STG.1		X				
FPT_STM.1						X

Table 4: Objectives implemented by SFRs

O.Admin is addressed by the following SFRs:

- FMT_SMR.1 requires the TOE to maintain separate Administrator roles
- FMT_SMF.1 specifies the management functions the TOE must provide
- FMT_MOF.1 restricts access to TOE management functions
- FMT_MSA.1 specifies which roles can access security attributes
- FMT_MTD.1 specifies which roles can access TSF data
- FDP_ACC.1/AdminCmd requires the TOE to enforce the Administrator Access Control SFP, and FDP_ACF.1/AdminCmd specifies the attributes used to enforce it
- FMT_MSA.3/VPNAccess defines static attribute initialization for the VPN Access Control SFP and who can modify the default values
- FMT_MSA.3/AdminCmd defines static attribute initialization for the Adminstrator Access Control SFP and who can modify the default values.

O.Audit is addressed by the following SFRs:

- 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 requires that the TOE provide the authorized administrators with the ability to read the audit records
- FAU_SAR.3 requires that the TOE provide the authorized administrators with the ability to search the audit records
- FAU_STG.1 requires that the TOE protect the audit records it holds.

O.Authenticate is addressed by FIA_UID.2 and FIA_UAU.2 which require Administrators to be identified and authenticated before they are able to perform any other actions.

O.IntAcc is addressed by the following SFRs:

- FIA_UID.2 requires VPN users to be identified before they are able to perform any other actions
- FIA_UAU.2 requires VPN users to be authenticated before they are able to perform any other actions
- FDP_ACC.1/VPNAccess requires the TOE to enforce the VPN Access Control SFP and FDP_ACF.1/VPNAccess specifies the attributes used to enforce it

- FDP_IFC.1/IntRes requires the TOE to enforce the VPN Information Flow Control SFP and FDP_IFF.1/IntRes specifies the attributes used to enforce it

- FMT_MSA.3/IntRes defines static attribute initialization for the VPN Information Flow Control SFP and who can modify the default values

- FMT_MSA.3/VPNAccess defines static attribute initialization for the VPN Access Control SFP and who can modify the default values.

O.ExtAcc is addressed by FDP_IFC.1/Traffic which requires the TOE to enforce the Web Application Firewall Information Flow Control SFP, FDP_IFF.1/Traffic which specifies the attributes used to enforce it, and FMT_MSA.3/Traffic which defines static attribute initialisation for the Web Application Firewall Information Flow Control SFP and who can modify the default values.

O.Time is addressed by FPT_STM.1 which requires that the TOE provide reliable timestamps for its own use.

5.4.2 SFR Dependencies Analysis

The dependencies between SFRs implemented by the TOE are addressed as follows.

SFR	Dependencies	Rationale Statement
FIA_UID.2	None	
FIA_UAU.2	FIA_UID.1	Met by FIA_UID.2 (hierarchical to FIA_UID.1)
FDP_ACC.1/AdminCmd	FDP_ACF.1	Met by FDP_ACF.1/AdminCmd
FDP_ACF.1/AdminCmd	FDP_ACC.1	Met by FDP_ACC.1/AdminCmd
	FMT_MSA.3	Met by FMT_MSA.3/AdminCmd
FDP_ACC.1/VPNAccess	FDP_ACF.1	Met by FDP_ACF.1/VPNAccess
FDP_ACF.1/VPNAccess	FDP_ACC.1	Met by FDP_ACC.1/VPNAccess
	FMT_MSA.3	Met by FMT_MSA.3/VPNAccess
FDP_IFC.1/IntRes	FDP_IFF.1	Met by FDP_IFF.1/IntRes
FDP_IFF.1/IntRes	FDP_IFC.1	Met by FDP_IFC.1/IntRes
	FMT_MSA.3	Met by FMT_MSA.3/IntRes

SFR	Dependencies	Rationale Statement
FDP_IFC.1/Traffic	FDP_IFF.1	Met by FDP_IFF.1/Traffic
FDP_IFF.1/Traffic	FDP_IFC.1	Met by FDP_IFC.1/Traffic
	FMT_MSA.3	Met by FMT_MSA.3/Traffic
FMT_SMR.1	FIA_UID.1	Met by FIA/UID.2 (hierarchical to FIA_UID.1)
FMT_SMF.1	None	
FMT_MOF.1	FMT_SMR.1	Met by FMT_SMR.1
	FMT_SMF.1	Met by FMT_SMF.1
FMT_MSA.1	FDP_ACC.1 or FDP_IFC.1	Met by FDP_ACC.1/AdminCmd
	FMT_SMR.1	Met by FMT_SMR.1
	FMT_SMF.1	Met by FMT_SMF.1
FMT_MTD.1	FMT_SMR.1	Met by FMT_SMR.1
	FMT_SMF.1	Met by FMT_SMF.1
FMT_MSA.3/AdminCmd	FMT_MSA.1	Met by FMT_MSA.1
	FMT_SMR.1	Met by FMT_SMR.1
FMT_MSA.3/VPNAccess	FMT_MSA.1	Met by FMT_MSA.1
	FMT_SMR.1	Met by FMT_SMR.1
FMT_MSA.3/IntRes	FMT_MSA.1	Met by FMT_MSA.1
	FMT_SMR.1	Met by FMT_SMR.1
FMT_MSA.3/Traffic	FMT_MSA.1	Met by FMT_MSA.1
	FMT_SMR.1	Met by FMT_SMR.1
FAU_GEN.1	FPT_STM.1	Met by FPT_STM.1
FAU_SAR.1	FAU_GEN.1	Met by FAU_GEN.1

SFR	Dependencies	Rationale Statement
FAU_SAR.3	FAU_SAR.1	Met by FAU_SAR.1
FAU_STG.1	FAU_GEN.1	Met by FAU_GEN.1
FPT_STM.1	None	

Table 5: Analysis of SFR dependencies

6. TOE Summary Specification

6.1 Security Audit

Administrators access the TOE through the CLI. 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 superuser, or a custom allowed role) can read, modify or delete them. (FAU_STG.1)

The TOE provides the capability to read the audit records through the CLI. 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)

This aspect of NetScaler therefore implements FAU_GEN.1, FAU_SAR.1, FAU_SAR.3, FAU_STG.1, FMT_MTD.1, and FMT_SMF.1

6.2 User Data Protection

This aspect of NetScaler implements FDP_ACC.1/AdminCmd, FDP_ACF.1/AdminCmd, FDP_ACC.1/VPNAccess, FDP_ACF.1/VPNAccess, FDP_IFC.1/IntRes, FDP_IFF.1/IntRes, FDP_IFC.1/Traffic, FDP_IFF.1/Traffic, FIA_UAU.2, and FIA_UID.2. The security functions are described below, under headings corresponding to each SFP enforced.

6.2.1 Administrator Access Control SFP

The Administrator Access Control SFP is applied to administrators when they access the NetScaler through the CLI. (FDP_ACC.1/AdminCmd)

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/AdminCmd)

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/AdminCmd)

6.2.2 VPN Access Control SFP

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

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/VPNAccess, 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/VPNAccess)

6.2.3 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/IntRes)

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/IntRes)

6.2.4 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/Traffic)

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/Traffic)

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/Traffic)

6.3 Identification and Authentication

Administrators access the TOE through the CLI. 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)

This aspect of NetScaler implements FIA_UAU.2 and FIA_UID.2.

6.4 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 the Security Management Matrix (see Table 2). (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 6.2 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/AdminCmd, FMT_MSA.3/VPNAccess, FMT_MSA.3/IntRes, FMT_MSA.3/Traffic)

This aspect of NetScaler therefore implements FMT_MOF.1, FMT_MSA.1, FMT_MSA.3/AdminCmd, FMT_MSA.3/VPNAccess, FMT_MSA.3/IntRes, FMT_MTD.3/Traffic, FMT_MTD.1, FMT_SMF.1, and FMT_SMR.1.

6.5 Timestamps

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)

This aspect of NetScaler implements FPT_STM.1.

End of Document