Nortel Networks
VPN Router v7.05 and Client Workstation v7.11

Security Target

Evaluation Assurance Level: EAL 4+
Document Version: 3.9

Prepared for:

Nortel Networks
600 Technology Park Drive
Billerica, MA 01821
Phone: (800) 466-7835
http://www.nortel.com

Prepared by:

Corsec Security, Inc.
10340 Democracy Lane, Suite 201
Fairfax, VA 22030
Phone: (703) 267-6050
http://www.corsec.com

Revision History

Version	Modification Date	Modified By	Description of Changes
1.0	2005-05-31	Kiran Kadambari	Initial draft.
2.0	2006-01-17	Nathan Lee	Revised to use new document layout; addressed lab verdicts; other miscellaneous edits to all sections for accuracy, consistency, flow, and readability.
2.1	2006-09-04	Christie Kummers	Revised dependencies for SFRs. Minor updates throughout.
3.0	2006-09-29	Christie Kummers	Minor updates throughout.
3.1	2006-10-25	Nathan Lee	Minor updates throughout.
3.2	2006-12-19	Christie Kummers	Updates and changes in response to Lab verdicts.
3.3	2007-3-02	Christie Kummers Nathan Lee	Updates and changes in response to Lab verdicts.
3.4	2007-06-04	Christie Kummers	Updates and changes in response to Lab verdicts.
3.5	2008-02-05	Nathan Lee	Updated TOE version number and responded to several lab verdicts.
3.6	2008-02-12	Nathan Lee	Updated TOE version build numbers.
3.7	2008-02-21	Nathan Lee	Updates and changes in response to Lab verdicts.
3.8	2008-03-18	Nathan Lee and Matt Keller	Updates based on lab verdict clarifications and FIPS validation details.
3.9	2008-03-18	Nathan Lee	Updated FIPS certificate numbers on 2009-01-21. Marked document publication/revision date as “2008-03-18” by request of CSEC.

Table of Contents

Table of Figures

Table of Tables

1 Security Target Introduction

This section identifies the Security Target (ST), Target of Evaluation (TOE) identification, ST conventions, ST conformance claims, and the ST organization. The Targets of Evaluation are models 600, 1010, 1050, 1100, 1750, 2750, and 5000 of the Nortel VPN Router v7.05 and Client Workstation v7.11. These devices are functionally identical and will hereafter be referred to, collectively, as "the TOE" throughout this document. The TOE is a Virtual Private Network (VPN) Router that ensures end-to-end network security by establishing a fully encrypted and authenticated VPN connection across the Internet between a Nortel VPN Router and either a user's remote computer or another remote Nortel VPN Router. It also provides firewall functionality to protect the private network from attack from the public network.

1.1 Purpose

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

- Security Target Introduction (Section 1) – Provides a brief summary of the content of the ST and describes the organization of other sections of this document.
- TOE Description (Section 2) – Provides an overview of the TOE security functions and describes the physical and logical boundaries for the TOE.
- 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.
- IT 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 to satisfy the security 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 as 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	Nortel Networks VPN Router v7.05 and Client Workstation v7.11 Security Target
ST Version	Version 3.8
Author	Corsec Security, Inc. Nathan Lee
TOE Identification	Nortel VPN Router v7.05 and Client Workstation v7.11
Common Criteria (CC) Identification and Conformance	Common Criteria for Information Technology Security Evaluation, Version 2.3 (aligned with ISO/IEC 15408:2004), Part 2 conformant, Part 3 conformant; Parts 2 and 3 Interpretations from the Interpreted CEM as of October 25, 2006 were reviewed, and no interpretations apply to the claims made in this ST.
PP Identification	None
Evaluation Assurance Level	EAL 4 Augmented with Flaw Remediation

Keywords	VPN, Router, Firewall, IPSec

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 several operations to be performed on security requirements: assignment, refinement, selection and iteration. All of these operations are used within this ST. These operations are presented in the same manner in which they appear in Parts 2 and 3 of the CC with the following exceptions:

- Completed assignment statements are identified using [*italicized text within brackets*].
- Completed selection statements are identified using [*underlined italicized text within brackets*].
- Refinements are identified using **bold text**. Any text removed is stricken (Example: ~~TSF Data~~) and should be considered as a refinement.
- Iterations are identified by appending a letter in parenthesis 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 Terminology

The acronyms used within this ST are described in Section 9 – "Acronyms." TOE-specific terminology used throughout the Security Target is explained in Table 2 below:

Table 2 - Terminology

Term	Explanation
Technology	
Contivity	Refers to the marketing name of the Nortel VPN Router.
User Types	
Primary Admin	The *Primary Admin* account has the ability to conduct all administrative privileges and rights of the TOE. The *Primary Admin* also has the ability to create and assign various rights to additional administrators. There can only be one *Primary Admin* of the TOE.
Restricted Admin	A *Restricted Admin* of the TOE has various administrative privileges as assigned by the *Primary Admin*. The types of privileges available to *Restricted Admins* are: • *Manage Nortel VPN Router* • *View Nortel VPN Router* • *Subgroups* • *Manage Users* • *View Users*
Administrators	Refers to all administrators of the TOE (both the *Primary Admin* and any assigned *Restricted Admins*)
Users	Refers to VPN users or any person authorized to use the TOE but lacking administrative privileges.
Operators	Refers to any human that interacts with the TOE, including *Administrators* and *Users*.
Privilege Types	

Term	Explanation
Manage Nortel VPN Router	Grants administrative rights to view (monitor) and manage (configure) Nortel VPN Router configuration settings or user rights settings. This is the highest level of administrative privilege. The only permission not granted to this level is access to the *Primary Admin* password.
View Nortel VPN Router	Grants administrative rights to view (monitor) most Nortel VPN Router configuration settings or user rights settings; however, this user cannot manage (change) them. This user cannot view the System Log, Graphs, and Guided Configuration.
Subgroups	Grants rights to add and delete subgroups under a directory for which the user has *View Nortel VPN Router* rights.
Manage Users	Grants administrative rights to view (monitor) and manage (configure) all group information for specified user groups.
View Users	Grants administrative rights to view (monitor) all group information for specified user groups.
None	The user does not have administrative rights to view (monitor) or manage (configure) the Nortel VPN Router settings or to manage user settings.

2 TOE Description

This section provides a general overview of the TOE as an aid to understanding the general capabilities and security requirements provided by the TOE. The TOE description provides a context for the TOE evaluation by identifying the product type and describing the evaluated configuration.

2.1 Product Type

The Nortel VPN Router v7.05 and Client Workstation v7.11 is a hardware and software TOE which combines network data routing, Virtual Private Network (VPN) connection and acceleration, and firewall capabilities in one device. This product class makes use of public telecommunication infrastructure (most commonly the Internet) in order to connect physically discontiguous private network segments to one "virtually contiguous" private network. Privacy and security of corporate data is maintained through the use of encrypted tunneling protocols within the VPN connection and various other security procedures when it is in transit over the public network.

A VPN connection requires the creation and operation of a secure tunnel between a VPN client on a remote device (such as personal computer (PC)) and VPN server software on a VPN security gateway, such as a Nortel VPN Router.

2.2 Product Description

The TOE is a VPN Router/Firewall which provides three main areas of functionality: it efficiently routes network traffic to its intended destination; it enables secure Internet Protocol (IP) VPN connections across the public data network; and it protects the private network from attack by parties on the public network. Each of these functions are discussed in greater detail below.

The TOE's primary purpose is to allow users of a private (Enterprise) network to have secure access to that network from a remote location. The TOE provides firewall, routing, encryption and decryption, authentication, and data integrity services to ensure that data is securely tunneled across IP networks (including the Internet). The Nortel VPN Router and the Nortel VPN Client are the two components that compose the TOE. Figure 1 below shows a typical deployment configuration of the TOE:

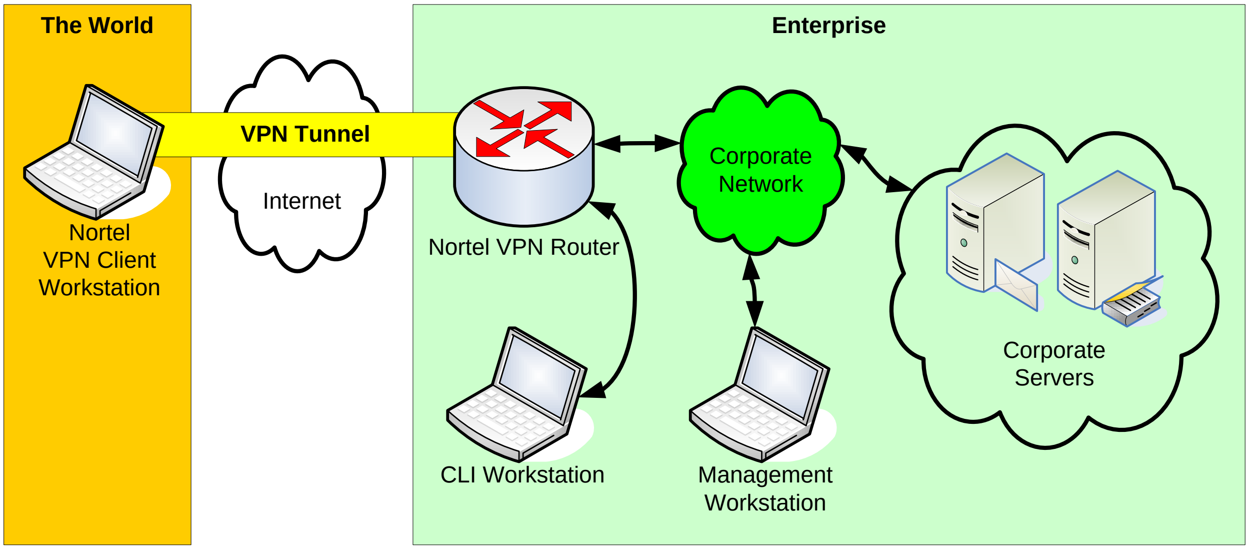

Figure 1 – VPN Client Deployment Configuration of the TOE

The Nortel VPN Router can also be configured to operate in Branch Office mode. Branch Office mode allows two separate portions of an Enterprise network to be securely connected to each other via the Internet. In Branch Office mode, a Nortel VPN Router on one Enterprise network segment will establish a VPN tunnel with another Nortel VPN Router on another Enterprise network segment. All communications between the two network segments are protected by the VPN tunnel. Figure 2 below shows a typical deployment configuration for Branch Office mode:

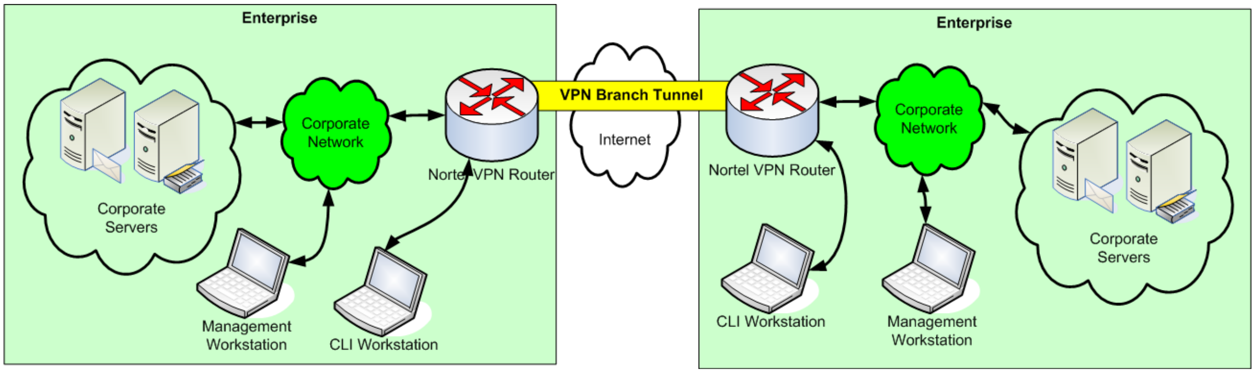

Figure 2 – Branch Office Deployment Configuration of the TOE

VPN sessions between the TOE components (the Nortel VPN Client and the Nortel VPN Router) can be established using various tunneling protocols, including L2TP, L2F, PPTP, and/or IP Security (IPSec); however, IPSec is the only tunneling protocol that can be used to establish a VPN session in the Common Criteria (CC) mode of operation. For this reason, IPSec is the only tunneling protocol that is discussed in detail in this Security Target document. Although a thorough discussion and analysis of the IPSec protocol is beyond the scope of this document, a brief description of the protocol is given below.

The IPSec protocol is designed to mitigate security threats to IP datagrams in three main areas: "spoofing" of IP addresses; IP datagram tampering and/or replaying; and IP datagram confidentiality. IPSec provides these security services at the Open Systems Interconnection (OSI) Network Layer (which is the layer containing the IP protocol) via combinations of cryptographic protocols and other security mechanisms. IPSec enables systems to dynamically select and require certain security protocols and cryptographic algorithms, and generate and utilize the cryptographic material (*i.e.*, keys) required to provide the requested services. These services include:

- Access control to network elements
- Data origin authentication
- Integrity for connection-less protocols (such as User Datagram Protocol (UDP))
- Detection and rejection of replayed IP packets (*i.e.* IP datagrams)
- Data confidentiality via encryption
- Partial traffic-flow confidentiality

These services are available for transparent use by any protocols which operate at higher levels in the OSI network stack.[1]

The TOE also provides stateful inspection firewall functionality which protects the private network from attack by parties on the public network. The firewall inspects the packets flowing through the router and uses administrator-configurable rules to determine whether or not to allow each packet to pass through to its intended destination.

TOE users fall into two groups:

1) Users who have access to the administrative functionality of the TOE.
2) Users who can only establish a VPN session with the TOE in order to have access to the network protected by the TOE.

[1] Davis, Carlton R. *IPSec: Securing VPNs*. RSA Press, 2001.

Configuration of the TOE is performed via a Command Line Interface (CLI) by physically connecting a device (such as a laptop) to the serial interface of the TOE and utilizing dumb-terminal software. After the TOE is configured, it can be managed remotely via a Graphical User Interface (GUI) which is accessed by a management workstation connected to the protected and trusted internal network.

2.3 TOE Boundaries and Scope

This section identifies the physical and logical components of the TOE that are included in this evaluation.

2.3.1 Physical Boundary

Figure 3 and Figure 4 below illustrates the physical boundary of this CC evaluation:

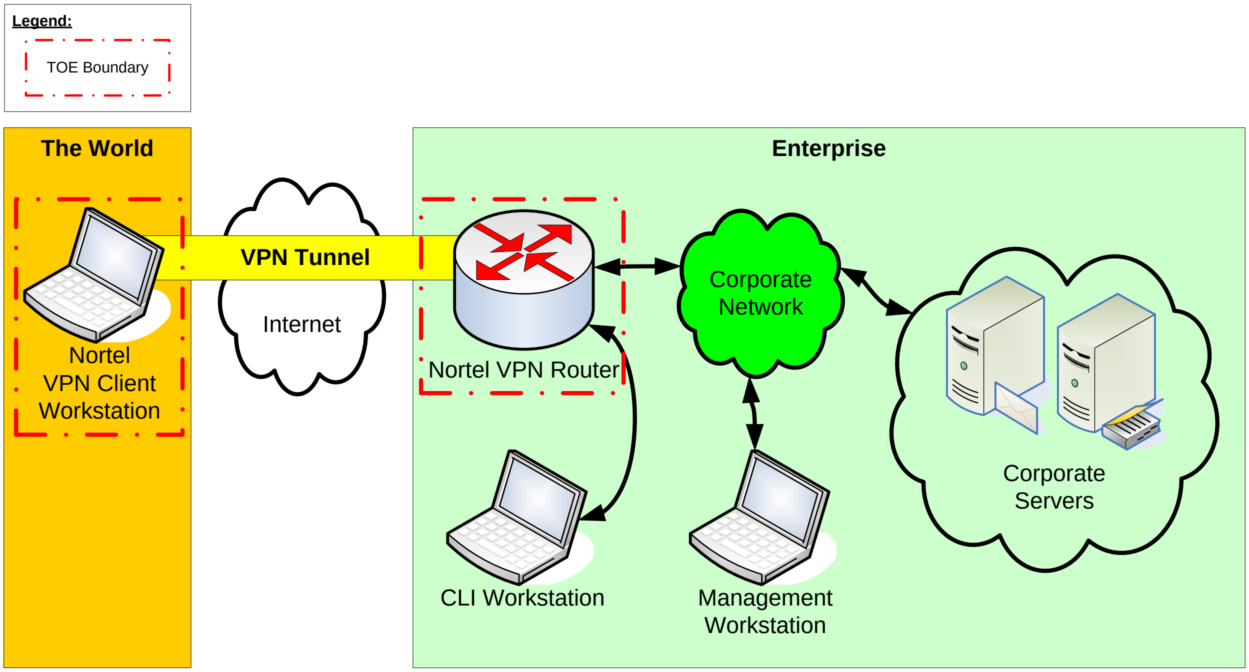

Figure 3 - Physical TOE Boundary

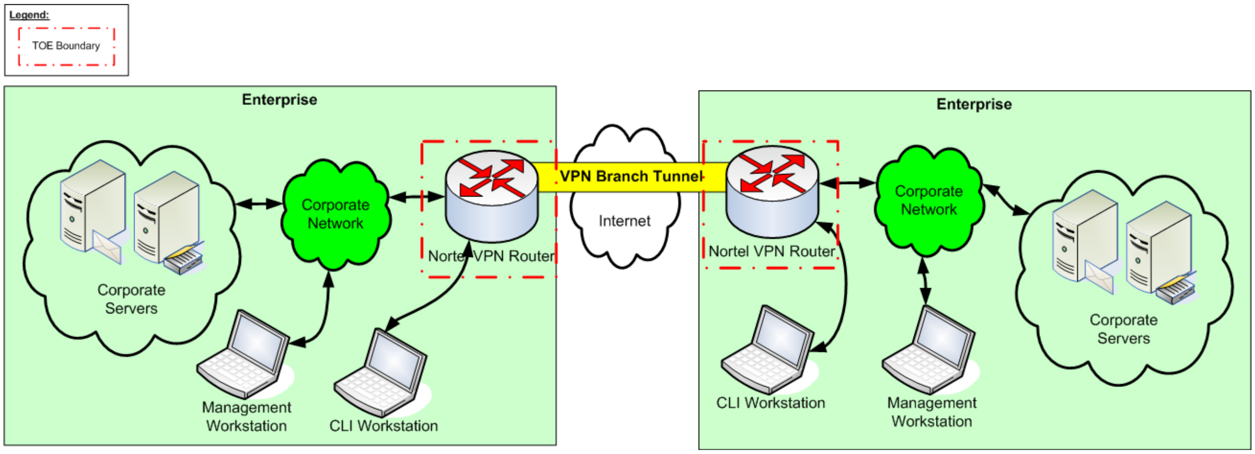

Figure 4 - Physical TOE Boundary in Branch Office Tunnel Mode

In Figure 3 above, the TOE is installed at the boundary of the private ("Enterprise") network and the public ("Internet") network. In Figure 4 above, the TOE is installed at the boundary of the two private ("Enterprise") networks. The essential physical components of the TOE are:

- **Nortel VPN Router v7.05 build 100:** The Nortel VPN Router is a dedicated hardware/software appliance running a Nortel-hardened version of the VxWorks OS. All non-essential OS processes have been removed and direct access to the OS is impossible. The Nortel VPN Router is produced at seven performance levels (models 600, 1010, 1050, 1100, 1750, 2750, and 5000) which provide identical functionality; they differ only in network throughput and performance.

- **Nortel VPN Client Workstation v7.11 build 100:** The Nortel VPN Client is used to access to establish VPN sessions with the Nortel VPN Router from a remote location.

2.3.1.1 TOE Environment

The TOE environment is composed of the following:

- Nortel VPN Client Workstation[2]
  - Provides the underlying OS (Microsoft Windows 2000 SP4 or XP SP2) and general-purpose computing hardware platform for the VPN user to connect to the Nortel VPN Router.
- Management Workstation
  - Provides the underlying OS and general-purpose computing hardware platform for the TOE user to interact with the administrative GUI provided by the TOE.
- CLI Workstation
  - Provides the underlying OS and general-purpose computing hardware platform for the TOE user to interact with the administrative CLI provided by the TOE.
- Corporate Servers
  - Provide data and services to VPN users through the VPN services provided by the TOE.

2.3.2 Logical Boundary

Figure 5 and Figure 6 below illustrates the logical boundary of this CC evaluation:

[2] Note that the Nortel VPN Client Software is included within the TOE boundary but the underlying OS and hardware are not.

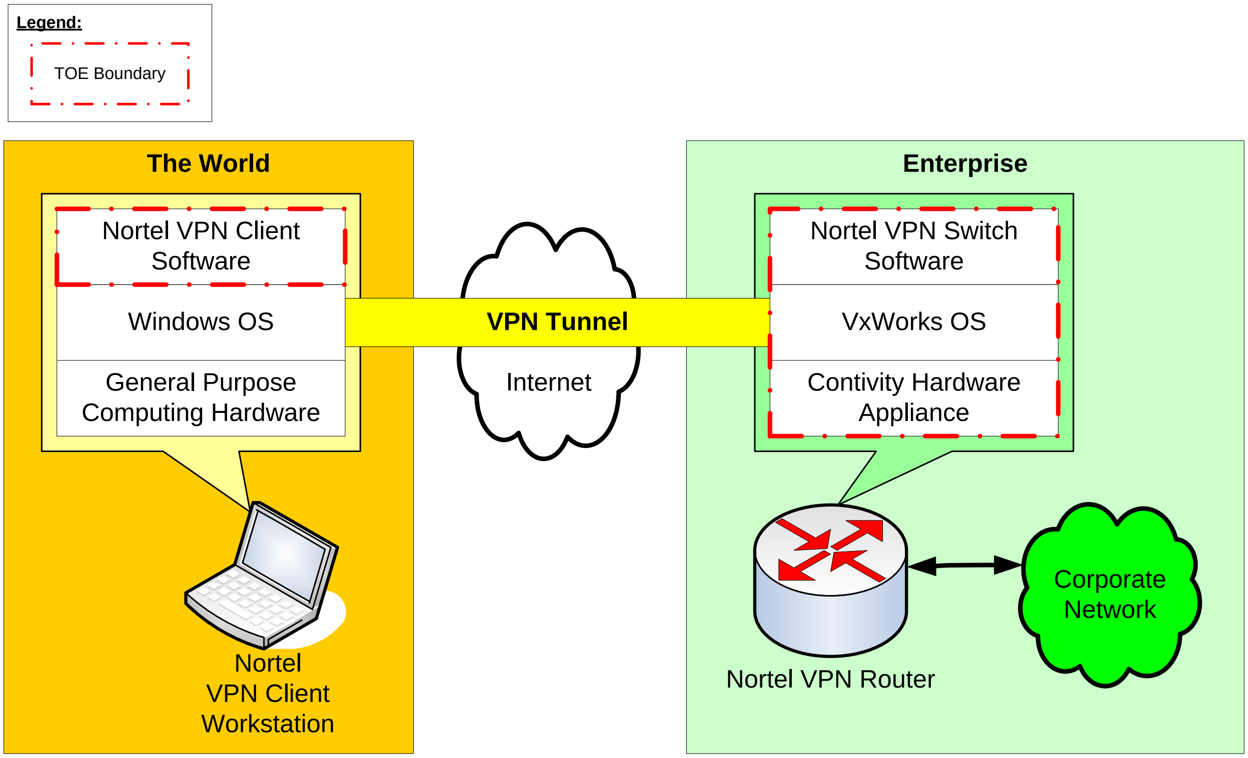
Legend:
TOE Boundary
The World
Nortel VPN Client Software
Windows OS
General Purpose Computing Hardware
Nortel VPN Client Workstation
VPN Tunnel
Internet
Enterprise
Nortel VPN Switch Software
VxWorks OS
Contivity Hardware Appliance
Nortel VPN Router
Corporate Network

Figure 5 - TOE Logical Boundary

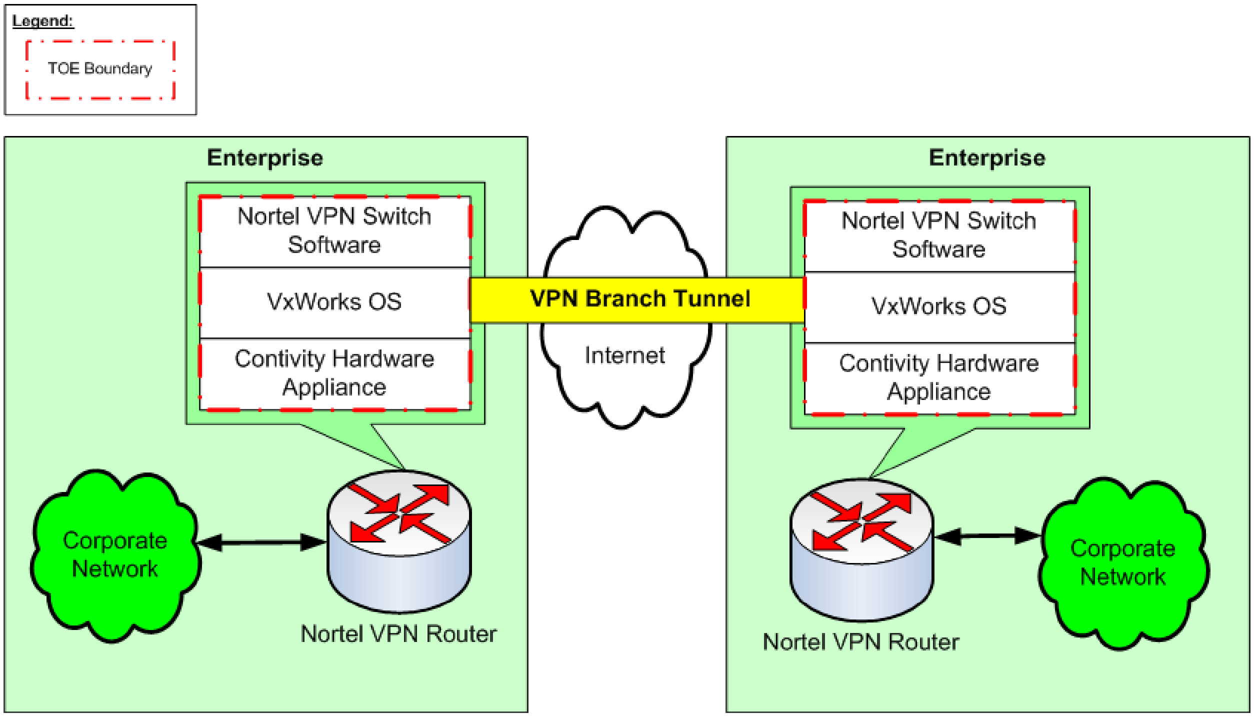

Figure 6 - TOE Logical Boundary in Branch Office Tunnel Mode

The essential logical components of the TOE are:

- **Nortel VPN Router:** Each of the logical components contained within the physical Nortel VPN Router are included within the TOE boundary. These components are:
    - Nortel VPN Switch Software
    - VxWorks OS
    - Contivity Hardware Appliance.

- **Nortel VPN Client Workstation:** The Nortel VPN Client software is part of the TOE but the underlying OS and hardware are excluded from the TOE boundary.

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

FAU	Security Audit
FCS	Cryptographic Support
FDP	User Data Protection
FIA	Identification and Authentication
FMT	Security Management
FPT	Protection of the TOE Security Functions
FTP	Trusted Path/Channels

These functions are discussed in greater detail below.

2.3.2.1 Security Audit

The Security Audit function provides the generation and viewing of audit records. The TOE generates five categories of audit data:

- **Accounting Log:** contains information about user activities.
- **Security Log:** contains information about security relevant activities.
- **Configuration Log:** contains information about configuration relevant activities.
- **System Log:** contains information about system relevant activities.
- **Event Log:** contains the last 2000 logs entries of all activities.

Audit data is generated by the TOE and stored locally as flat files on internal storage. The TOE controls access to the audit data, and direct access to these flat files by the TOE administrator is not possible. The TOE supports automatic backup and archiving of the logs.

TOE users assigned to the appropriate user roles may read audit records but do not have write access. The audit data is presented to TOE users in a manner suitable for human readability.

2.3.2.2 Cryptographic Support

The TOE implements and utilizes cryptographic algorithms and various other security algorithms in order to protect information being transferred between physically separated parts of the TOE. These algorithms include Advanced Encryption Standard (AES), Triple Data Encryption Standard (3DES), RSA (Rivest, Shamir, and Adleman), and Diffie-Hellman; Secure Hash Algorithm (SHA-1) and Keyed-Hash Message Authentication Code (HMAC)-SHA-1 for hashing; and FIPS 140-2 key zeroization for key destruction.

2.3.2.3 User Data Protection

The TOE enforces the Access Control Security Functional Policy (SFP) on TOE subjects, objects, and operations. The architecture of the TOE ensures that all operations between objects and subjects are regulated by the TOE based upon the privilege criteria defined in the Access Control SFP.

The TOE enforces the VPN Information Flow Control (IFC) SFP and the Firewall IFC SFP through the use of IPSec. The IPSec protocol ensures confidentiality of communications between remote Nortel VPN Clients and

Nortel VPN Routers, as well as providing protection against external attack. The architecture of the TOE ensures that VPN data is subject to enforcement of the VPN IFC SFP, and that all data passing through the firewall is subject to enforcement of the Firewall IFC SFP. These SFPs are enforced by the TOE based upon the privilege criteria defined in the SFPs.

2.3.2.4 Identification and Authentication

All identification and authentication for the TOE occurs on the Nortel VPN Router and is based on user attributes. Each user has a username, password, and one or more assigned roles. The TOE ensures that users are authenticated prior to any use of the TOE functions, and user authentication is performed using a unique username and password combination.

TOE users must identify and authenticate their identities in order to gain access to services provided by the TOE. Identification and authentication is enforced by the Nortel VPN Router, the GUI, and the CLI. The Nortel VPN Client accepts two types of authentication credentials: a username/password combination or a digital certificate.[3] The GUI and CLI accepts username/password authentication.

2.3.2.5 Security Management

The TOE maintains three main user roles:

- Primary Admin
- Restricted Admin
- VPN User

The Primary Admin has full administrative access to the TOE; the Restricted Admin has access to specific administrative functions as defined by the Primary Admin; and the VPN User has no administrative privileges and can only connect to the Nortel VPN Router via the Nortel VPN Client.

The Primary Admin and Restricted Admins perform administrative and troubleshooting tasks via the GUI, and they perform configuration tasks via the CLI. VPN Users utilize the Nortel VPN Client to access the private network through the Nortel VPN Router. After successful authentication to the TOE, users can access only the management functions to which their role grants them access. As described in the SFP, management and modification of TOE security attributes is restricted to authorized administrators in order to ensure that only secure values are accepted for those security attributes and that the default values used for initialization of the security attributes are not maliciously altered.

2.3.2.6 Protection of the TOE Security Functions

The TOE runs a series of self-tests both at initial TOE start-up and periodically during normal TOE operation. These tests check for the correct operation of the TSFs. The TOE is able to detect IPSec sessions replay attacks and take appropriate countermeasures (by dropping the suspect packets) while performing the self-tests. The TOE's architecture is specifically designed to eliminate the possibility of any user bypassing the TSFs. Users must be identified and authenticated before the TOE will make any actions on their behalf. The underlying OS is not accessible by any TOE user (authorized or unauthorized).

2.3.2.7 Trusted Path/Channels

Connections from the Nortel VPN Client to the Nortel VPN Router are initiated by the VPN Users. IPSec is required during these connections in order to ensure that the communication is via a trusted path. The architecture of the TOE and of the IPSec protocol ensures that the trusted paths between the Nortel VPN Router and the Nortel VPN Clients are logically distinct and secure.

[3] The Nortel VPN Client also supports the use of Smart Cards for authentication. Smart Card authentication is beyond the scope of this evaluation and is not included in the evaluated configuration.

2.3.3 Excluded TOE Functionality

The following product features and functionality are excluded from the evaluated configuration of the TOE:

- Remote VPN connections using a tunneling protocol other than IPSec
- Remote authentication using a Smart Card or a hardware or software token Card

3 TOE 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. Section 3.1 provides assumptions about the secure usage of the TOE, including physical, personnel, and connectivity aspects. Section 3.2 lists the known and presumed threats countered by either the TOE or by the security environment.

3.1 Assumptions

This section contains assumptions regarding the security environment and the intended usage of the TOE. 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.

A.TRAINED-ADMIN It is assumed that administrators will be trained in the secure use of the TOE and will follow the policies and procedures defined in the TOE documentation for secure administration of the TOE. Administrators are assumed to be non-hostile.

A.TIMESTAMPS It is assumed that the TOE relies on the operating environment of TOE to provide accurate clock time in order to create an accurate time stamp for audit events. Administrators are responsible for the maintenance of a reliable time source for use with audit operations.

A.PHYSICAL It is assumed that the TOE may be susceptible to physical attacks by an attacker. It is assumed that the TOE will be housed within a physically secure environment in order to mitigate this risk.

A.CERTIFICATE It is assumed that the environment will provide the necessary infrastructure to ensure that certificates can be validated when digital certificates are used for authentication. This may mean the environment provides a connection to a trusted Certificate Authority, or that the required certificates are otherwise available to the TOE. It is assumed that the appropriate infrastructure is properly maintained in order to ensure the accuracy and security of the certificates (*e.g.*, certificates are revoked in a timely manner).

A.INSTALL It is assumed that the TOE is delivered, installed, and setup in accordance with documented delivery and installation/setup procedures.

A.ACCESS It is assumed that the TOE has access to all of the Information Technology (IT) System data it needs to perform its functions.

A.DOMSEP It is assumed that the IT environment will maintain a security domain for the Nortel VPN software that protects it from interference and tampering by untrusted subjects.

3.2 Threats to Security

This section identifies the threats to the IT assets (private networks) 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:** These attackers have no knowledge of how the TOE operates and are assumed to possess a low skill level, a low level of motivation, limited resources to alter TOE configuration settings/parameters, and no physical access to the TOE.
- **TOE users:** These attackers have extensive knowledge of how the TOE operates and are assumed to possess a high skill level, moderate resources to alter TOE configuration settings/parameters, and physical access to the TOE, but no motivation to do so.

The threats are mitigated through the objectives identified in Section 4 - Security Objectives.

3.2.1 Threats Addressed by the TOE

The following threats are to be addressed by the TOE:

T.UNDETECT An attacker may gain undetected access due to missing, weak, and/or incorrectly implemented access controls for the restricted files or TSF Data in order to cause violations of integrity, confidentiality, or availability of the information protected by and flowing through the TOE.

T.AUTH-ERROR An authorized user may accidentally alter the configuration of a policy that permits or denies information flow through the TOE, thereby affecting the integrity of the transmitted information.

T.DATA-MOD An attacker may intercept and alter the data transmitted between the Nortel VPN Client and the Nortel VPN Router, and/or between two Nortel VPN Routers, in order to deceive the intended recipient.

T. HACK-CRYPTO An attacker may successfully intercept and decrypt, then recover and modify the encrypted data that is in transit between the Nortel VPN Router and VPN Client, and/or between two Nortel VPN Routers.

T.HACK An attacker may use malformed IP packets or similar attack methods against the TSF or user data protected by the TOE in order to corrupt normal operation.

3.2.2 Threats Addressed by the TOE Environment

The following threats are addressed by the TOE environment:

TE.PHYSICAL An attacker may physically attack the Hardware appliance in order to compromise its secure operation.

TE.AUDIT_FAILURE An attacker may conduct an undetected attack on the information protected by the TOE as a result of unreliable time stamps used by the audit mechanism, which may result in failure to prevent further attacks using the same method.

TE.BAD_CERT An attacker may successfully authenticate to the VPN Router using a revoked, expired or untrusted certificate in order to gain access to information residing on the private network.

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 in meeting the security needs.

4.1 Security Objectives for the TOE

The specific security objectives are as follows:

O.I&A The TOE must be able to identify and authenticate users prior to allowing access to TOE functions and data.

O.AUDIT The TOE must record audit records for data accesses and use of the System functions.

O.SELFPROTECT The TOE must protect itself from unauthorized modifications and access to its functions and data.

O.FUNCTIONS The TOE must provide functionality that enables only authorized users to establish VPN sessions with the TOE using the IPSec protocol.

O.ADMIN The TOE must provide facilities to enable an authorized administrator to effectively manage the TOE and its security function, and must ensure that only authorized administrators are able to access such functionality.

O.TEST The TOE must provide functionality that enables testing of its correct functioning and integrity.

O.REPLAY The TOE must provide functionality that enables detection of replay attack and take appropriate action if an attack is detected.

O.CONFIDENT The TOE must use the IPSec tunneling protocol to ensure confidentiality of data transmitted between the Nortel VPN Client and the Nortel VPN Router, and/or between two Nortel VPN Routers.

O.INTEGRITY The TOE must use the IPSec tunneling protocol to ensure integrity of data transmitted between the Nortel VPN Client and the Nortel VPN Router, and/or between two Nortel VPN Routers.

O.FILTER The TOE must filter all incoming and outgoing packets that pass through it, and accept or reject packets based on their attributes.

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:

OE.TIME The environment must provide reliable timestamps for the time-stamping of audit events.

OE.CERTIFICATE The environment must provide the required certificate infrastructure so that the validity of certificates can be verified. The certificate infrastructure must be properly and securely maintained so that the status of certificates is accurately provided to the TOE.

OE.DOMSEP The environment must maintain a security domain for the Nortel VPN Client software that protects it from interference and tampering by untrusted subjects.

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.

OE.PHYS-SEC The TOE must be physically protected so that only TOE users who possess the appropriate privileges have access.

OE.TRAINED Those responsible for the TOE must train TOE users to establish and maintain sound security policies and practices.

OE.DELIVERY Those responsible for the TOE must ensure that it is delivered, installed, managed and operated in accordance with documented delivery and installation/setup procedures.

5 IT Security Requirements

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

5.1 TOE Security Functional Requirements

This section specifies the SFRs for the TOE. This section organizes the SFRs by CC class. Table 3 identifies all SFRs implemented by the TOE and indicates the ST operations performed on each requirement.

Table 3 - TOE Security Functional Requirements

SFR ID	Description	ST Operation			
		Selection	Assignment	Refinement	Iteration
FAU_GEN.1	Audit Data Generation	✓	✓		
FAU_SAR.1	Audit Review		✓		
FCS_CKM.1(a)	Cryptographic Key Generation		✓		
FCS_CKM.4	Cryptographic Key Destruction		✓		
FCS_COP.1(a)	Cryptographic Operation		✓		✓
FCS_COP.1(b)	Cryptographic Operation		✓		✓
FCS_COP.1(d)	Cryptographic Operation		✓		✓
FCS_COP.1(e)	Cryptographic Operation		✓		✓
FCS_CKM.1(b)	Cryptographic Key Generation		✓		
FDP_ACC.2	Complete Access Control		✓		
FDP_ACF.1	Security Attribute Based Access Control		✓		
FDP_IFC.2(a)	Complete Information Flow Control		✓		✓
FDP_IFC.2(b)	Complete Information Flow Control		✓		✓
FDP_IFF.1(a)	Simple Security Attributes		✓		✓
FDP_IFF.1(b)	Simple Security Attributes		✓		✓
FDP_UCT.1	Basic Data Exchange Confidentiality	✓	✓		
FDP_UIT.1	Data Exchange Integrity	✓	✓		
FIA_UAU.1	Timing of Authentication		✓		
FIA_UAU.5	Multiple Authentication Mechanisms		✓		
FIA_UID.2	User Identification Before any Action				
FMT_MOF.1(a)	Management of Security Functions Behavior	✓	✓		✓
FMT_MOF.1(b)	Management of Security Functions Behavior	✓	✓		✓
FMT_MSA.1(a)	Management of Security Attributes	✓	✓		✓

SFR ID	Description	ST Operation			
FMT_MSA.1(b)	Management of Security Attributes	✓	✓		✓
FMT_MSA.1(c)	Management of Security Attributes	✓	✓		✓
FMT_MSA.2	Secure Security Attributes				
FMT_MSA.3(a)	Static Attribute Initialization	✓	✓		✓
FMT_MSA.3(b)	Static Attribute Initialization	✓	✓		✓
FMT_MSA.3(c)	Static Attribute Initialization	✓	✓		✓
FMT_SMF.1	Specification of Management Functions		✓		
FMT_SMR.1	Security Roles		✓		
FPT_AMT.1	Abstract Machine Testing	✓			
FPT_RPL.1	Replay Detection		✓		
FPT_TST.1	TSF Testing	✓	✓		
FTP_TRP.1	Trusted Path	✓	✓		

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.

5.1.1 Class FAU: Security Audit

FAU_GEN.1 Audit Data Generation

Hierarchical to: No other components.

FAU_GEN.1.1

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

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

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

c) [*All events listed in Table 4*].

Table 4 - Auditable Events

Event
Start-up and shutdown of audit functions
Modification to the TSF and System data
Reading of information from the audit Records
All modifications to the audit configuration that occur while the audit collection functions are operating
All use of the user identification and authentication mechanism
All modifications in the behavior of the Functions of the TSF
Modifications to the role allocation of users

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, [*no other audit relevant information*].

Dependencies: FPT_STM.1 Reliable time stamps

FAU_SAR.1 Audit review

Hierarchical to: No other components.

FAU_SAR.1.1

The TSF shall provide [*Primary Admin, the Restricted Admin, and the VPN User*] with the capability to read [*all audit records that they have permission to view*] 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

5.1.2 Class FCS: Cryptographic Support

FCS_CKM.1(a) Cryptographic key generation (Diffie-Hellman)

Hierarchical to: No other components.

FCS_CKM.1.1(a)

The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [*Diffie-Hellman*] and specified cryptographic key sizes [*1024, 1536 bit keys*] that meet the following: [*RFC 2631*].

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

FCS_CKM.1(b) Cryptographic key generation (RSA)

Hierarchical to: No other components.

FCS_CKM.1.1(b)

The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [*RSA*] and specified cryptographic key sizes [*1024, 2048 bits*] that meet the following: [*RFC 3447*].

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

FCS_CKM.4 Cryptographic key destruction

Hierarchical to: No other components.

FCS_CKM.4.1

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

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

FCS_COP.1(a) Cryptographic operation (encryption and decryption)

Hierarchical to: No other components.

FCS_COP.1.1(a)

The TSF shall perform [*encryption and decryption*] in accordance with a specified cryptographic algorithm [*3DES and AES*] and cryptographic key sizes [*168-bit key, 128 and 256-bit keys, respectively*] that meet the following: [*FIPS 46-3 and FIPS 197, respectively*].

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

FCS_COP.1(b) Cryptographic operation (authentication)

Hierarchical to: No other components.

FCS_COP.1.1(b)

The TSF shall perform [*authentication*] in accordance with a specified cryptographic algorithm [*HMAC-SHA-1*] and cryptographic key sizes [*512-bits*] that meet the following: [*RFC 2104*].

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

FCS_COP.1(d) Cryptographic operation (random number generation)

Hierarchical to: No other components.

FCS_COP.1.1(d)

The TSF shall perform [*random number generation*] in accordance with a specified cryptographic algorithm [*SHA-1*] and cryptographic key sizes [*20 bytes*] that meet the following: [*FIPS 186-2 Appendix 3.1*].

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

FCS_COP.1(e) Cryptographic operation (hashing)

Hierarchical to: No other components.

FCS_COP.1.1(e)

The TSF shall perform [*hashing*] in accordance with a specified cryptographic algorithm [*SHA-1*] and cryptographic key sizes [*none*] that meet the following: [*RFC 3174*].

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

5.1.3 Class FDP: User Data Protection

FDP_ACC.2 Complete access control

Hierarchical to: FDP_ACC.1

FDP_ACC.2.1

The TSF shall enforce the [*Access Control SFP*] on [*Subjects: administrators; Objects: VPN Router configuration parameters*] and all operations among subjects and objects covered by the SFP.

FDP_ACC.2.2

The TSF shall ensure that all operations between any subject in the TSC and any object within the TSC are covered by an access control SFP.

Dependencies: FDP_ACF.1 Security attribute based access control

FDP_ACF.1 Security attribute based access control

Hierarchical to: No other components.

FDP_ACF.1.1

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

FDP_ACF.1.2

The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [*if an administrator has been authenticated, if that administrator has privileges granted by the Primary Admin*].

FDP_ACF.1.3

The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [*access to all administrative functions is permitted once a Primary Admin has been identified and authenticated successfully*].

FDP_ACF.1.4

The TSF shall explicitly deny access of subjects to objects based on [*no additional explicit denial rules*].

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

FDP_IFC.2(a) Complete information flow control (VPN)

Hierarchical to: FDP_IFC.1

FDP_IFC.2.1(a)

The TSF shall enforce the [*VPN Information Flow Control SFP*] on [*remote authenticated VPN Clients connecting to a Nortel VPN Router*] and all operations that cause that information to flow to and from subjects covered by the SFP.

FDP_IFC.2.2(a)

The TSF shall ensure that all operations that cause any information in the TSC to flow to and from any subject in the TSC are covered by an information flow control SFP.

Dependencies: FDP_IFF.1 Simple security attributes

FDP_IFC.2(b) Complete information flow control (Firewall)

Hierarchical to: FDP_IFC.1

FDP_IFC.2.1(b)

The TSF shall enforce the [*Firewall Information Flow Control SFP*] on [*hosts on either side of a Nortel VPN Router (subject), and the Nortel VPN Router (subject), and all data flowing between the subjects (information)*] and all operations that cause that information to flow to and from subjects covered by the SFP.

FDP_IFC.2.2(b)

The TSF shall ensure that all operations that cause any information in the TSC to flow to and from any subject in the TSC are covered by an information flow control SFP.

Dependencies: FDP_IFF.1 Simple security attributes

FDP_IFF.1(a) Simple security attributes (VPN)

Hierarchical to: No other components.

FDP_IFF.1.1(a)

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

- *user identity,*
- *user authentication credentials*

and tunnel filtering of packets is based on

- *Protocol ID,*
- *Direction,*
- *Source, destination IP addresses,*
- *Source, destination ports,*
- *Service*].

FDP_IFF.1.2(a)

The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: [*the VPN Client successfully authenticates to the Nortel VPN Router*].

FDP_IFF.1.3(a)

The TSF shall enforce the [*none*].

FDP_IFF.1.4(a)

The TSF shall provide the following [*stateful Firewall, Network Address Translation (NAT), IPSec*].

FDP_IFF.1.5(a)

The TSF shall explicitly authorise an information flow based on the following rules: [*none*].

FDP_IFF.1.6(a)

The TSF shall explicitly deny an information flow based on the following rules: [*none*].

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

FDP_IFF.1(b) Simple security attributes (Firewall)

Hierarchical to: No other components.

FDP_IFF.1.1(b)

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

- *Source, destination interface;*
- *Source, destination IP addresses;*
- *Source, destination port;*
- *Direction*
- *Service*].

FDP_IFF.1.2(b)

The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: [*attempted connection from external source has an entry in the state-based connection table permitting its inflow*].

FDP_IFF.1.3(b)

The TSF shall enforce the [*none*].

FDP_IFF.1.4(b)

The TSF shall provide the following [*stateful Firewall, Network Address Translation (NAT)*].

FDP_IFF.1.5(b)

The TSF shall explicitly authorise an information flow based on the following rules: [*none*].

FDP_IFF.1.6(b)

The TSF shall explicitly deny an information flow based on the following rules: [*if packet sequence number indicates repeated packet, signaling a replay attack*].

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

FDP_UCT.1 Basic data exchange confidentiality

Hierarchical to: No other components.

FDP_UCT.1.1

The TSF shall enforce the [*VPN Information Flow Control SFP*] to be able to [*transmit, receive*] objects in a manner protected from unauthorised disclosure.

Dependencies: [FTP_ITC.1 Inter-TSF trusted channel, or
FTP_TRP.1 Trusted path]
[FDP_ACC.1 Subset access control, or
FDP_IFC.1 Subset information flow control]

FDP_UIT.1 Data exchange integrity

Hierarchical to: No other components.

FDP_UIT.1.1

The TSF shall enforce the [*VPN Information Flow Control SFP*] to be able to [*transmit, receive*] user data in a manner protected from [*modification, deletion, insertion, replay*] errors.

FDP_UIT.1.2

The TSF shall be able to determine on receipt of user data, whether [*modification, deletion, insertion, replay*] has occurred.

Dependencies: [FDP_ACC.1 Subset access control, or
FDP_IFC.1 Subset information flow control]
[FTP_ITC.1 Inter-TSF trusted channel, or
FTP_TRP.1 Trusted path]

5.1.4 Class FIA: Identification and Authentication

FIA_UAU.1 Timing of authentication

Hierarchical to: No other components.

FIA_UAU.1.1

The TSF shall allow [

- ○ *connection configuration,*
- ○ *username entry,*
- ○ *password entry,*
- ○ *destination selection,*
- ○ *authentication options (digital certificates, username, password),*
- ○ *keepalive options,*
- ○ *autoconnect,*
- ○ *name server options*

] on behalf of the user to be performed before the user is authenticated.

FIA_UAU.1.2

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_UAU.5 Multiple authentication mechanisms

Hierarchical to: No other components.

FIA_UAU.5.1

The TSF shall provide [*username and password (for administrators), RSA Digital Certificates*] to support user authentication.

FIA_UAU.5.2

The TSF shall authenticate any user's claimed identity according to the [*configurations as defined by administrators and these configurations include:*

- ○ *Username and Password (for administrators)*
- ○ *RSA Digital Certificates*].

Dependencies: No dependencies

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[4] TSF-mediated actions on behalf of that user.

Dependencies: No dependencies

[4] "Other" in this SFR means any action not included in the assignment in FIA_UAU.1.1.

5.1.5 Class FMT: Security Management

FMT_MOF.1(a) Management of security functions behaviour

Hierarchical to: No other components.

FMT_MOF.1.1(a)

The TSF shall restrict the ability to [*modify the behaviour of*] the functions [*creation and rights assignment of Restricted Admins*] to [*Primary Admin*].

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

FMT_MOF.1(b) Management of security functions behaviour

Hierarchical to: No other components.

FMT_MOF.1.1(b)

The TSF shall restrict the ability to [*determine the behaviour of*] the functions [*all administrator functions allowed by Primary Admin*] to [*Restricted Admins*].

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

FMT_MSA.1(a) Management of security attributes

Hierarchical to: No other components.

FMT_MSA.1.1(a)

The TSF shall enforce the [*Access Control SFP*] to restrict the ability to [*modify*] the security attributes [*which includes all internal attributes available to the administrators*] to [*Primary Admin, Restricted Admins*].

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.1(b) Management of security attributes

Hierarchical to: No other components.

FMT_MSA.1.1(b)

The TSF shall enforce the [*Firewall Information Control SFP*] to restrict the ability to [*modify*] the security attributes [*which includes all internal attributes available to the administrators*] to [*Primary Admin, Restricted Admins*].

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.1(c) Management of security attributes

Hierarchical to: No other components.

FMT_MSA.1.1(c)

The TSF shall enforce the [*VPN Information Control SFP*] to restrict the ability to [*modify*] the security attributes [*which includes all internal attributes available to the administrators*] to [*Primary Admin, Restricted Admins*].

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

FMT_MSA.2 Secure security attributes

Hierarchical to: No other components.

FMT_MSA.2.1

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

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

FMT_MSA.3(a) Static attribute initialisation

Hierarchical to: No other components.

FMT_MSA.3.1(a)

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

FMT_MSA.3.2(a)

The TSF shall allow the [*Primary Admin*] to specify alternative initial values to override the default values when an object or information is created.

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

FMT_MSA.3(b) Static attribute initialisation

Hierarchical to: No other components.

FMT_MSA.3.1(b)

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

FMT_MSA.3.2(b)

The TSF shall allow the [*Primary Admin*] to specify alternative initial values to override the default values when an object or information is created.

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

FMT_MSA.3(c) Static attribute initialisation

Hierarchical to: No other components.

FMT_MSA.3.1(c)

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

FMT_MSA.3.2(c)

The TSF shall allow the [*Primary Admin*] to specify alternative initial values to override the default values when an object or information is created.

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

FMT_SMF.1 Specification of Management Functions

Hierarchical to: No other components.

FMT_SMF.1.1

The TSF shall be capable of performing the following security management functions: [*Management of creation of roles and assigning rights, determining the administrator functions, management of Access Control policies, management of Firewall and VPN information flow policies, management of audit records, management of cryptographic functions, performing self tests*].

Dependencies: No Dependencies

FMT_SMR.1 Security roles

Hierarchical to: No other components.

FMT_SMR.1.1

The TSF shall maintain the roles [*Primary Admin, Restricted Admin, VPN User*].

FMT_SMR.1.2

The TSF shall be able to associate users with roles.

Dependencies: FIA_UID.1 Timing of identification

5.1.6 Class FPT: Protection of the TSF

FPT_AMT.1 Abstract machine testing

Hierarchical to: No other components.

FPT_AMT.1.1

The TSF shall run a suite of tests [*during initial start-up, periodically during normal operation*] to demonstrate the correct operation of the security assumptions provided by the abstract machine that underlies the TSF.

Dependencies: No dependencies

FPT_RPL.1 Replay detection

Hierarchical to: No other components.

FPT_RPL.1.1

The TSF shall detect replay for the following entities: [*the IPSec sessions*].

FPT_RPL.1.2

The TSF shall perform [*drop packets*] when replay is detected.

Dependencies: No dependencies

FPT_TST.1 TSF testing

Hierarchical to: No other components.

FPT_TST.1.1

The TSF shall run a suite of self tests [*during initial start-up, at the conditions [when running in Normal mode]*] to demonstrate the correct operation of [*the TSF*].

FPT_TST.1.2

The TSF shall provide authorised users with the capability to verify the integrity of [*TSF data*].

FPT_TST.1.3

The TSF shall provide authorised users with the capability to verify the integrity of stored TSF executable code.

Dependencies: FPT_AMT.1 Abstract machine testing

5.1.7 Class FTP: Trusted Path/Channels

FTP_TRP.1 Trusted path

Hierarchical to: No other components.

FTP_TRP.1.1

The TSF shall provide a communication path between itself and [*remote*] users that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from modification or disclosure.

FTP_TRP.1.2

The TSF shall permit [*remote users*] to initiate communication via the trusted path.

FTP_TRP.1.3

The TSF shall require the use of the trusted path for [*[secure VPN communication]*].

Dependencies: No dependencies

5.2 Security Functional Requirements on the IT Environment

The TOE has the following security requirement for its IT environment. Table 5 identifies all SFRs implemented by the IT Environment and indicates the ST operations performed on each requirement.

Table 5 - IT Environment Security Functional Requirements

SFR ID	Description	ST Operation			
		Selection	Assignment	Refinement	Iteration
FPT_RVM.1	Non-bypassability of the TSP			✓	
FPT_SEP.1	TSF domain separation			✓	
FPT_STM.1	Reliable time stamps			✓	

FPT_RVM.1 Non-bypassability of the TSP

Hierarchical to: No other components.

FPT_RVM.1.1

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

Dependencies: No dependencies

FPT_SEP.1 TSF domain separation

Hierarchical to: No other components.

FPT_SEP.1.1

The ~~TSF~~ **IT Environment** shall maintain a security domain for ~~its own~~ **the TOE's** execution that protects ~~it~~ **the TOE** 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~~ **TOE Environment** shall be able to provide reliable time stamps for ~~it's~~ **the TOE's** own use.

Dependencies: No dependencies

5.3 Assurance Requirements

This section defines the assurance requirements for the TOE. The assurance requirements are taken from Part 3 of the CC and are EAL 4 augmented with ALC_FLR.2. Table 6 below summarizes the components.

Table 6 - Assurance Components

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

6 TOE Summary Specification

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

6.1 TOE Security Functions

Each of the security function descriptions is organized by the security requirements corresponding to the security function. 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 are suitable to satisfy the necessary requirements.

Table 7 - Mapping of TOE Security Functions to Security Functional Requirements

TOE Security Function	SFR ID	Description
Security Audit	FAU_GEN.1	Audit Data Generation
	FAU_SAR.1	Audit Review
Cryptographic Support	FCS_CKM.1(a)	Cryptographic Key Generation
	FCS_CKM.1(b)	Cryptographic Key Generation
	FCS_CKM.4	Cryptographic Key Destruction
	FCS_COP.1(a)	Cryptographic Operation
	FCS_COP.1(b)	Cryptographic Operation
	FCS_COP.1(d)	Cryptographic Operation
	FCS_COP.1(e)	Cryptographic Operation
User Data Protection	FDP_ACC.2	Complete Access Control
	FDP_ACF.1	Security Attribute Based Access Control
	FDP_IFC.2(a)	Complete Information Flow Control
	FDP_IFC.2(b)	Complete Information Flow Control
	FDP_IFF.1(a)	Simple Security Attributes
	FDP_IFF.1(b)	Simple Security Attributes
	FDP_UCT.1	Basic Data Exchange Confidentiality
	FDP_UIT.1	Data Exchange Integrity
Identification and Authentication	FIA_UAU.1	Timing of Authentication
	FIA_UAU.5	Multiple Authentication Mechanisms
	FIA_UID.2	User Identification Before any Action
Security Management	FMT_MOF.1(a)	Management of Security Functions Behavior
	FMT_MOF.1(b)	Management of Security Functions Behavior
	FMT_MSA.1(a)	Management of Security Attributes
	FMT_MSA.1(b)	Management of Security Attributes
	FMT_MSA.1(c)	Management of Security Attributes
	FMT_MSA.2	Secure Security Attributes
	FMT_MSA.3(a)	Static Attribute Initialization

TOE Security Function	SFR ID	Description
	FMT_MSA.3(b)	Static Attribute Initialization
	FMT_MSA.3(c)	Static Attribute Initialization
	FMT_SMF.1	Specification of Management Functions
	FMT_SMR.1	Security Roles
Protection of the TSF	FPT_AMT.1	Abstract Machine Testing
	FPT_RPL.1	Replay Detection
	FPT_TST.1	TSF Testing
Trusted Path/Channels	FTP_TRP.1	Trusted Path

6.1.1 Security Audit

The TOE generates five types of audit data:

Accounting Logs The Accounting Log records the following data about user sessions:

- Last name
- First name
- User ID
- Tunnel type
- Session start date
- Session end date
- Number of packets transferred
- Number of bytes transferred

Security Log The Security Log records data about both successful and failed system and user security events. The audited events include:

- Authentication and authorization events
- Tunnel or administration requests
- Encryption and decryption, authentication, or compression
- Hours of access
- Number of session violations
- Communications with servers
- LDAP
- RADIUS

Configuration Log The Configuration Log records data about configuration changes, including the addition, modification, or deletion of:

- Group or user profiles
- Local Area Network (LAN or Wide Area Network (WAN) interfaces
- Filters
- System access hours
- Shutdown or startup policies
- File maintenance or backup policies

System Log

The System Log records data about System events which are considered significant enough to be written to disk, including those displayed in the Configuration and Security logs. Examples of events that would appear in the System log include:

- LDAP activity
- Configuration activity
- Server authentication and authorization requests

The following list gives the general format of System Log entries:

- Time stamp
- Task that issued the event (“tEvtLgMgr”, “tObjMgr”, “tHttpdTask”)
- A number that indicates the Central Processing Unit (CPU) that issued the event (“0” = “CPU(0)”, “1” = “CPU(1)”)
- Software module that issued the event
- A number that indicates the event’s persistence (“0” = “non-persistent”, “1” = “persistent”)
- A number that indicates the event’s severity level (“0” = “Debug”, “1” = “Low”, “2” = “Medium”, “3” = “High”)
- Rule section matched by this event
- Matching packet source, destination, protocol, and action configured for the matched rule

Event Log

The Event Log records detailed data about all events that take place on the system. These entries are not necessarily written to disk (as with the System Log). The Event Log records data about all system activity in-memory, but only the significant entries are saved in the System Log (*i.e.*, on disk).

The Event Log includes information on tunneling, security, backups, debugging, hardware, security, daemon processes, software drivers, interface card driver events, and other system components and event types.

The Event Log retains the most recent 2000 log entries. Once this maximum capacity has been reached the Event Log overwrites the oldest entry when a new entry needs to be made.

TOE administrators interact with the TOE through the management GUI [or CLI], but unprivileged TOE users are restricted to establishing VPN sessions with the TOE via the Nortel VPN Client. All of the user actions (detailed above) performed through either of these interfaces are recorded in the appropriate audit log. The TOE creates an audit record when a TOE user causes any of the events in “Table 4 - Auditable Events” to occur. Audit records generated in the Nortel VPN Router are stored locally as flat files on internal storage with no direct TOE administrator access.

Since audit functionality is critical to the secure operation of the TOE, both internal and external backups of the audit logs are supported. Automatic backup and archiving of the logs ensures that the logs are always available. External storage backup of audit records occurs outside of the TOE and it is the administrator’s responsibility to specify an external backup server.

TOE administrators may view audit records via a management GUI display (in a manner suitable for human consumption and understanding). This display includes the date and time of the event; the type of event; the subject identity; the outcome (success or failure) of the event; and the identity of the user responsible for the event. TOE users can read audit records only through the TOE’s management GUI, and only after being authenticated to an appropriately privileged role. TOE users are never given write access to the audit records.

TOE Security Functional Requirements Satisfied: FAU_GEN.1, FAU_SAR.1.

6.1.2 Cryptographic Support

The TOE's cryptographic functionality is provided by a FIPS 140-2-validated cryptographic module. All modules have received either a Level 1 or Level 2 FIPS 140-2 validation. Table 8 below indicates the modules and the validation levels achieved.

Table 8 - FIPS Validated Modules

Validation	Modules	FIPS 140-2 Certificate #
Hardware modules FIPS 140-2 validated at level 2	VPN Router 1750, 2700, 2750 and 5000 with Hardware Accelerator	1068
	VPN Router 1750, 2700, 2750 and 5000 with VPN Router Security Accelerator	1073
	Nortel VPN Router 600, 1750, 2700, 2750 and 5000	1066
Hardware modules FIPS 140-2 validated at level 1	Nortel VPN Router 1010, 1050 and 1100	1067
Software module being validated at level 1 of FIPS 140-2:	VPN Client Software	1032

The TOE's cryptographic module implements and utilizes the following FIPS-validated cryptographic algorithms:

Table 9 - FIPS-Validated Cryptographic Algorithms

Algorithm	Key Size(s) (bits)	Validated Against	FIPS Certificate #
3DES	168	FIPS 46-3	641, 642, 644
AES	128, 256	FIPS 197	718, 719, 721
RSA[5]	1024, 2048	FIPS 186-2	338, 339
SHA-1	N/A	FIPS 180-2	738, 739, 740
HMAC-SHA-1	160	FIPS 198[6]	387, 388, 389

The TOE generates RSA keys for signature generation and verification. During the key generation process, all weak keys are discarded. The resultant strong RSA keys are used to perform key agreement and authentication in accordance with the Diffie-Hellman and IKE protocols.

The TOE performs encryption and decryption using the 3DES and AES algorithms. The TOE implements the HMAC-SHA-1 algorithm in order to perform data origin authentication and data integrity checks upon encrypted packets entering the TOE. The TOE implements SHA-1 algorithm in order to perform data integrity checks upon encrypted packets entering the TOE.

The TOE destroys keys when they are no longer needed by "zeroizing" them. Zeroization is performed by overwriting the memory location containing the keys with zeros before marking the memory location as being free

[5] Via the RSA BSAFE library.
[6] FIPS 198 is equivalent to RFC 2104.

for reuse. This ensures that the keys are completely destroyed before any other process might have access to that memory location.

TOE Security Functional Requirements Satisfied: FCS_CKM.1(a), FCS_CKM.1(b), FCS_CKM.4, FCS_COP.1(a), FCS_COP.1(b)., FCS_COP.1(d), FCS_COP.1(e)

6.1.3 User Data Protection

The TOE enforces access controls on each administrator and user of the TOE based on the privileges held by that user.

Access Control SFP: The TOE enforces the Access Control SFP on administrators by assigning privileges to administrators. The TOE configuration parameters can only be modified by those administrative users granted permission to do so by the Primary Admin. Administrators (specifically Restricted Admins) have a restricted level of access based on the permissions granted to them by the Primary Admin. Details of these privilege levels can be found in Section 2.3.2.5. All administrators must be authenticated before access is granted. The Primary Admin has access to all administrative functions after successfully being identified and authenticated to the TOE.

VPN Information Flow Control SFP: The TOE enforces the VPN Information Flow Control SFP by allowing connections only from VPN Clients who authenticate to the remote Nortel VPN Router (via the Nortel VPN Client) with either a username/password combination or via a digital certificate. The VPN Information Flow Control SFP is also enforced based on user identity and authentication credentials. The VPN Information Flow Control SFP enforces session tunnel filtering based on a packets protocol ID, direction, source and destination IP addresses, source and destination ports, and service.

The TSF enforces the VPN Information Flow Control SFP on user data in order to protect sent or received data from modification, deletion, insertion, or replay. Thus, the TSF can determine if the data has been modified, deleted, inserted, or replayed via the VPN Information Flow Control SFP.

The connection attributes configured in the Nortel VPN Router enable the remote user to create a tunnel into the Nortel VPN Router. The actual connection to the Nortel VPN Router is a tunnel that is started from the remote user’s PC, through the public network, and ends at the Nortel VPN Router on the private network. The Nortel VPN Router associates all remote users with a group which dictates the attributes (and privileges) that are assigned to a remote user session.

The VPN Information Flow Control SFP enforces the IPSec protocol for establishing a VPN. The VPN session that is established by remote users creates a trusted communications path between the remote user and the TOE. This communications path is logically distinct from other paths due to the cryptography that is used to encrypt the trusted session.

The TOE supports “split-tunneling,” which assigns a unique IP address to an established IPSec tunnel, which is different than (and is held simultaneously with) the IP address assigned to the host machine which established the tunnel. During split-tunneling, any packet sent from the host machine to the public network must have as its source address the IP address assigned to the tunnel. Any packet sent to the public network with the host’s IP address (or any other address) as the source address is dropped. For example, a user’s host might have an IP address of 192.168.21.3. This user might then establish an IPSec connection with a host on the public network. This IPSec tunnel might be assigned a tunnel IP address of 192.192.192.192. In this case, any packets that attempt to pass outward through the tunnel with a source IP address of 192.168.21.3 (or any address other than 192.192.192.192) are dropped.

Firewall Information Flow Control SFP: The TOE enforces the Firewall Information Flow Control SFP by allowing connections only from hosts on either side of a Nortel VPN Router. The Firewall Information Flow Control SFP is also enforced on packets based on their source and destination interface, source and destination IP addresses, source and destination ports, direction, and service.

The TOE’s Firewall examines both incoming and outgoing packets and compares them to a security policy. If the packet sequence numbers indicate a repeated packet, the TOE drops the packets as an identified replay attack.

VPN Information Flow Control SFP and Firewall Information Flow Control SFP: Both SFPs enforce a stateful Firewall. Each time a TCP connection is established from a host on the internal network to a host on the external network through the Nortel VPN Router, information about the connection is recorded in a stateful session flow table. The state table contains the source and destination addresses and port number(s) for each TCP connection associated with that particular host. This information creates a connection object in the Nortel VPN Router. Inbound packets are compared against session flows in the connection table and are permitted through the Nortel VPN Router only if an appropriate connection already exists to validate their passage. This connection object is terminated when the session is finished.

Both SFPs enforce Network Address Translation (NAT) functionality which helps to provide transparent routing between private IP address spaces. NAT allows the dynamic connection of multiple private networks via secure tunnels without requiring any address space reconfiguration. The NAT policy is configured by administrators either via the GUI or the CLI. The NAT policy in the TOE is associated with a security property and a security policy. The security property defines the type of service offered (including the service name, the protocol (TCP, UDP, ICMP), and the port number (or range) on which the service occurs). The security policy is a set of rules that specifies which service is allowed or denied.

Within the Nortel VPN Router, the source address of a packet is translated after the packet has gone through the Nortel VPN Router if a matching source NAT rule is found. A NAT policy consists of one or more NAT rules. A NAT rule describes the translation action to take for a particular source, destination, or service. NAT is applied to routed traffic passing through the TOE's physical interfaces using separate NAT policies. The NAT policy is retrieved from the LDAP database after system initialization and packets are processed according to the NAT policy rules.

TOE Security Functional Requirements Satisfied: FDP_ACC.2, FDP_ACF.1, FDP_IFC.2(a), FDP_IFC.2(b), FDP_IFF.1(a), FDP_IFF.1(b), FDP_UCT.1, FDP_UIT.1.

6.1.4 Identification and Authentication

Users of the TOE can access it in three ways: via the Nortel VPN Client, the CLI, or the GUI. Users are processed and authorized by the TOE's identification and authentication mechanism whenever they access any of these interfaces. TOE users can authenticate to the CLI and the management GUI by providing a valid username and its corresponding password. TOE users can authenticate to the Nortel VPN Client by providing either a valid username and its corresponding password or a valid digital certificate.[7] Cryptographic functions relevant to the use of digital certificates are discussed in Section 6.1.2. Prior to identification and authentication of a user via the Nortel VPN Client, TOE users are given the opportunity to choose one of these authentication methods. This action (choosing an authentication method) can not be used by an attacker to disrupt the proper functioning of the TOE.

The TOE stores a username, a hashed password, and the roles associated with the user, for each TOE user in order to enable authentication via username/password. A user is authenticated when the hash of the password that has been entered matches the stored hashed password. The username/password authentication mechanism is the only implemented probabilistic security mechanism. In the CC mode of operation, the minimum required password length for users is eight characters (with a possible character set of at least 94 characters), which meets the Strength of Function (SOF) claim of SOF-basic.

TOE Security Functional Requirements Satisfied: FIA_UAU.1, FIA_UAU.5, FIA_UID.2.

6.1.5 Security Management

The TOE maintains three roles, the Primary Admin, the Restricted Admin, and the VPN User. The Primary Admin has full access to the TOE. The Restricted Admins have only the permissions granted to them by the Primary Admin. Permissions granted to the Restricted Admin by the Primary Admin may include access to administrative

[7] See Footnote 3 for more information.

functions. The VPN User has no access to administrative functions and may only authenticate to the Nortel VPN Router through the Nortel VPN Client in order to access the private network.

These roles determine a user's level of access to security management functions provided by the TOE. These security management functions include management of all audit and event records, management of access control, and management of VPN and firewall functions. Each user assumes one role from the available roles.

Administrators manage TOE security functionality and change, query, modify, or delete security attributes via the management GUI. All requests for services from either the management GUI or the Nortel VPN Client are passed to the Nortel VPN Router, which mediates access control to those functions. The Nortel VPN Router makes the access control decision by comparing the user's role and the privilege requirement for the type of request made.

As described in the Security Functional Policies, management and modification of secure values are restricted to ensure that only secure values are accepted for security attributes and that the default values used for initialization of the security attributes are not altered.

TOE Security Functional Requirements Satisfied: FMT_MOF.1(a), FMT_MOF.1(b), FMT_MSA.1(a), FMT_MSA.1(b), FMT_MSA.1(c), FMT_MSA.2, FMT_MSA.3(a), FMT_MSA.3(b), FMT_MSA.3(c), FMT_SMF.1, FMT_SMR.1.

6.1.6 Protection of the TOE Security Functions

The TOE's FIPS 140-2 validated cryptographic module will offer its services only after all power-up self-tests (at power-up) and all conditional self-tests (when creation of an IPSec tunnel is requested) have passed; if these self-tests do not pass then the TOE enters an error state and logs the failure. All error states can be cleared by restarting the module. If the self-tests do pass, then an IPSec tunnel is established, thus activating all of the IPSec security features. The TOE runs continuous checks on the IPSec tunnel to detect replay attacks. If a replay attack is detected then the associated packets are immediately dropped.

The TOE performs the following Start-Up and Conditional Self-Tests in order to ensure the secure and proper operation of the TSF:

6.1.6.1 Power-Up Self-Tests

FIPS 140-2 validated power-up self-tests are executed automatically when the module is started. The Start-Up Self-Tests performed by the TOE are described below:

- **Software Integrity Check:** Verifies the integrity of the software binaries of the module using an HMAC-SHA-1 keyed hash.
- **AES Known Answer Test (KAT):** Verifies the correct operation of the AES algorithm implementation.
- **3DES KAT:** Verifies the correct operation of the Triple-DES algorithm implementation.
- **SHA-1 KAT:** Verifies the correct operation of the SHA-1 algorithm implementation.
- **HMAC-SHA-1 KAT:** Verifies the correct operation of the HMAC-SHA-1 algorithm implementation.
- **FIPS 186-2 Random Number Generator (RNG) KAT:** Verifies the correct operation of the FIPS 186-2 RNG implementation.
- **Alternating Bypass Mode Test:** Verifies the integrity of the module's bypass capability (hard-coded in the filter driver).

6.1.6.2 Conditional Self-Tests

FIPS 140-2 validated conditional self-tests are executed automatically when certain criteria or events occur. The TOE performs three conditional self-tests: a pair-wise consistency test each time the an RSA public/private key is generated, a continuous random number generator test each time the module produces random data, and a software load test for upgrades. The Conditional Self-Tests performed by the TOE are described below.

- **FIPS 186-2 Continuous RNG:** Verifies that the Approved RNG is not failing to a constant value.

  - Runs when a random number needs to be generated.
- **Continuous RNG for Entropy Gathering:** Verifies that the seed for the FIPS 182-2 PRNG is not failing to a constant value.
  - Runs when a seed for the RNG needs to be generated.
- **Pair-wise Consistency Test for RSA Key Generation:** Verifies that a newly generated RSA public/private keypair works properly.
  - Runs when an RSA public/private keypair is generated.
- **Software Load Test:** Verifies the authenticity and integrity of new software binaries which are to be installed on the module.
  - Runs when a new software image is loaded onto the module.

TOE Security Functional Requirements Satisfied: FPT_AMT.1, FPT_RPL.1, FPT_TST.1.

6.1.7 Trusted Path/Channels

Connections from the Nortel VPN Client to the Nortel VPN Router are initiated by the VPN users. IPSec is required to ensure that the communication is via trusted path. Because of this, trusted path connections between components of the TOE are logically distinct, and secure.

TOE Security Functional Requirements Satisfied: FTP_TRP.1.

6.2 TOE Security Assurance Measures

EAL 4 augmented with ALC_FLR.2 was chosen to provide a basic level of independently assured security. This section of the ST maps the assurance requirements of the TOE for a CC EAL 4+ (augmented with ALC_FLR.2) level of assurance to the assurance measures used for the development and maintenance of the TOE. The following table provides a mapping of the appropriate documentation to the TOE assurance requirements.

Table 10 - Assurance Measures Mapping to TOE Security Assurance Requirements (SARs)

Assurance Component	Assurance Measure
ACM_AUT.1	Nortel Networks Virtual Private Network Router v7.05 Configuration Management
ACM_CAP.4	Nortel Networks Virtual Private Network Router v7.05 Configuration Management
ACM_SCP.2	Nortel Networks Virtual Private Network Router v7.05 Configuration Management
ADO_DEL.2	Nortel Networks Virtual Private Network Router v7.05 Secure Delivery
ADO_IGS.1	Nortel Virtual Private Network Router v7.05 Installation Guidance
ADV_FSP.2	Nortel Networks Virtual Private Network Router v7.05 Functional Specification
ADV_HLD.2	Nortel Networks Virtual Private Network Router v7.05 TOE Architecture: High Level Design, Low Level Design, and Representation Correspondence
ADV_IMP.1	Nortel Networks Virtual Private Network Router v7.05 - Implementation Representation
ADV_LLD.1	Nortel Networks Virtual Private Network Router v7.05 TOE Architecture: High Level Design, Low Level Design, and Representation Correspondence
ADV_RCR.1	Nortel Networks Virtual Private Network Router v7.05 TOE Architecture: High Level Design, Low Level Design, and Representation Correspondence
ADV_SPM.1	Nortel Networks Virtual Private Network Router v7.05 Informal Security Policy Model
AGD_ADM.1	Nortel Networks Virtual Private Network Router v7.05 Supplement Guide
AGD_USR.1	Nortel Networks Virtual Private Network Router v7.05 Supplement Guide

Assurance Component	Assurance Measure
ALC_DVS.1	Nortel Networks Virtual Private Network Router v7.05 Life Cycle Support
ALC_FLR.2[8]	Nortel Networks Virtual Private Network Router v7.05 Life Cycle Support
ALC_LCD.1	Nortel Networks Virtual Private Network Router v7.05 Life Cycle Support
ALC_TAT.1	Nortel Networks Virtual Private Network Router v7.05 Life Cycle Support
ATE_COV.2	Nortel Networks Virtual Private Network Router v7.05 Functional, Coverage, and Depth Analysis
ATE_DPT.1	Nortel Networks Virtual Private Network Router v7.05 Functional, Coverage, and Depth Analysis
ATE_FUN.1	Nortel Networks Virtual Private Network Router v7.05 Functional, Coverage, and Depth Analysis
ATE_IND.2	[Performed by testing laboratory]
AVA_MSU.2	Nortel Networks Virtual Private Network Router v7.05 - Misuse
AVA_SOF.1	Nortel Networks Virtual Private Network Router v7.05 Vulnerability Analysis
AVA_VLA.2	Nortel Networks Virtual Private Network Router v7.05 Vulnerability Analysis

[8] Augmentation to EAL 4+ assurance level.

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 11 demonstrates the mapping between 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 11 - Relationship of Security Threats to Objectives

			TOE Objectives										Environmental Objectives					
													IT			Non-IT		
			O.I&A	O.AUDIT	O.SELFPROTECT	O.CONFIDENT	O.INTEGRITY	O.FILTER	O.FUNCTIONS	O.ADMIN	O.TEST	O.REPLAY	OE.TIME	OE.CERTIFICATE	OE.DOMSEP	OE.PHYS-SEC	OE.TRAINED	OE.DELIVERY
Threats	TOE	T.UNDETECT	✓	✓					✓		✓							
		T.AUTH-ERROR								✓	✓						✓	
		T.DATA-MOD			✓	✓	✓				✓	✓						
		T.HACK-CRYPTO			✓	✓	✓				✓	✓						
		T.HACK			✓			✓			✓	✓		✓				
	TOE Environment	TE.PHYSICAL														✓		
		TE.AUDIT_FAILURE											✓					
		TE.BAD_CERT							✓					✓				
Assumptions		A.TRAINED-ADMIN															✓	
		A.TIMESTAMPS											✓					
		A.PHYSICAL														✓		
		A.CERTIFICATE												✓				
		A.INSTALL																✓
		A.ACCESS																✓
		A.DOMSEP													✓			

T.UNDETECT An attacker may gain undetected access due to missing, weak, and/or incorrectly implemented access controls for the restricted files or TSF Data in order to cause violations of integrity, confidentiality, or availability of the information protected by and flowing through the TOE.

The TOE identifies and authenticates users prior to allowing access to TOE functions and data (O.I&A). The TOE records audit records for data accesses and use of the System functions (O.AUDIT). The TOE provides functionality that enables only authorized user to establish VPN sessions with the TOE using IPSec protocol (O.FUNCTIONS). The TOE provides functionality that enables testing of its correct functioning and integrity (O.TEST).

O.I&A, O.AUDIT, O.FUNCTIONS, and O.TEST combined ensure that this threat is removed.

T.AUTH-ERROR An authorized user may accidentally alter the configuration of a policy that permits or denies information flow through the TOE, thereby affecting the integrity of the transmitted information.

The TOE provide facilities to enable an authorized administrator to effectively manage the TOE and its security function, and ensures that only authorized administrators are able to access such functionality (O.ADMIN). The TOE provides functionality that enables testing of its correct functioning and integrity (O.TEST). Those responsible for the TOE train TOE users to establish and maintain sound security policies and practices (OE.TRAINED).

O.ADMIN, O.TEST, and OE.TRAINED combined ensure that this threat is removed.

T.DATA-MOD An attacker may intercept and alter the data transmitted between the Nortel VPN Client and the Nortel VPN Router, and/or between two Nortel VPN Routers, in order to deceive the intended recipient.

The TOE protects itself from unauthorized modifications and access to its functions and data (O.SELFPROTECT). The TOE uses IPSec tunneling protocol to ensure confidentiality and integrity of data transmitted between the Nortel VPN Client and the Nortel VPN Router, and/or between two Nortel VPN Routers (O.CONFIDENT & O.INTEGRITY). The TOE provides functionality that enables testing of its correct functioning and integrity (O.TEST). The TOE provides functionality that enables detection of replay attack and thus take action is a replay attack is detected (O.REPLAY).

O.SELFPROTECT, O.CONFIDENT, O.INTEGRITY, O.TEST, and O.REPLAY combined ensure that this threat is removed.

T. HACK-CRYPTO An attacker may successfully intercept and decrypt, then recover and modify the encrypted data that is in transit between the Nortel VPN Router and VPN Client, and/or between two Nortel VPN Routers.

The TOE protects itself from unauthorized modifications and access to its functions and data (O.SELFPROTECT). The TOE uses IPSec tunneling protocol to ensure confidentiality and integrity of data transmitted between the Nortel VPN Client and the Nortel VPN Router, and/or between two Nortel VPN Routers (O.CONFIDENT & O.INTEGRITY). The TOE provides functionality that enables testing of its correct functioning and integrity (O.TEST). The TOE provides functionality that enables detection of replay attack and thus take action is a replay attack is detected (O.REPLAY).

O.SELFPROTECT, O.CONFIDENT, O.INTEGRITY, O.TEST, O.REPLAY combined ensure that this threat is removed.

T.HACK An attacker may use malformed IP packets or similar attack methods against the TSF or user data protected by the TOE in order to corrupt normal operation.

The TOE protects itself from unauthorized modifications and access to its functions and data (O.SELFPROTECT). The TOE filters all incoming and outgoing packets that pass through it, and accepts or rejects transmissions based on their attributes (O.FILTER). The environment ensures that the required certificate infrastructure is provided so that the validity of certificates can be verified. The TOE provides functionality that enables testing of its correct functioning and integrity (O.TEST). The TOE provides functionality that enables detection of replay attack and thus take action is a replay attack is detected (O.REPLAY). The Environment also ensures that the chosen infrastructure is maintained so that certificates have their state accurately provided to the TOE (OE.CERTIFICATE).

O.SELFPROTECT, O.FILTER, O.TEST, O.REPLAY, and OE.CERTIFICATE combined ensure that this threat is removed.

TE.PHYSICAL An attacker may physically attack the Hardware appliance in order to compromise its secure operation.

The environment ensures that the TOE is physically protected so that only TOE users who possess the appropriate privileges have access (OE.PHYS-SEC).

OE.PHYS-SEC ensures that this threat is removed.

TE.AUDIT_FAILURE An attacker may conduct an undetected attack on the information protected by the TOE as a result of unreliable time stamps used by the audit mechanism, which may result in failure to prevent further attacks using the same method.

The environment ensures that reliable timestamps are provided for the time-stamping of audit events (OE.TIME).

OE.TIME ensures that this threat is removed.

TE.BAD_CERT An attacker may successfully authenticate to the VPN Router using a revoked, expired or untrusted certificate in order to gain access to information residing on the private network.

The environment ensures that the required certificate infrastructure is provided so that the validity of certificates can be verified. The Environment also ensures that the chosen infrastructure is maintained so that certificates have their state accurately provided to the TOE (OE.CERTIFICATE). The TOE provides functionality that enables only authorized user to establish VPN sessions with the TOE using IPSec protocol (O.FUNCTIONS).

OE.CERTIFICATE and O.FUNCTIONS ensure that this threat is removed.

A.TRAINED-ADMIN It is Assumed that administrators will be trained in the secure use of the TOE and will follow the policies and procedures defined in the TOE documentation for secure administration of the TOE. Administrators are assumed to be non-hostile.

Those responsible for the TOE ensure that the TOE users are trained to establish and maintain sound security policies and practices (OE.TRAINED).

OE.TRAINED satisfies this assumption.

A.TIMESTAMPS It is assumed that the TOE relies on the operating environment of TOE which provides the accurate clock time to maintain an accurate time stamp for audit events. Administrators are responsible for the maintenance of a reliable time source to provide accurate time for use with audit operations.

The environment ensures that reliable timestamps are provided for the time-stamping of audit events (OE.TIME).

OE.TIME satisfies this assumption.

A.PHYSICAL It is assumed that the TOE may be susceptible to physical attacks by an attacker. It is assumed that the TOE will be housed within a physically secure environment in order to mitigate this risk.

The environment ensures that the TOE is physically protected so that only TOE users who possess the appropriate privileges have access (OE.PHYS-SEC).

OE.PHYS-SEC satisfies this assumption.

A.CERTIFICATE It is assumed that the environment will provide the necessary infrastructure to ensure that certificates can be validated when digital certificates are used for authentication.

This may mean the environment provides a connection to a trusted Certificate Authority, or that the required certificates are otherwise available to the TOE. It is assumed that the appropriate infrastructure is properly maintained in order to ensure the accuracy and security of the certificates (*e.g.*, certificates are revoked in a timely manner).

The environment ensures that the required certificate infrastructure is provided so that the validity of certificates can be verified. The Environment also ensures that the chosen infrastructure is maintained so that certificates have their state accurately provided to the TOE (OE.CERTIFICATE).

OE.CERTIFICATE satisfies this assumption.

A.INSTALL **It is assumed that the TOE is delivered, installed, and setup in accordance with documented delivery and installation/setup procedures.**

Those responsible for the TOE ensure that it is delivered, installed, managed, and operated in accordance with documented delivery and installation/setup procedures (OE.DELIVERY).

OE.DELIVERY satisfies this assumption.

A.ACCESS **It is assumed that the TOE has access to all the IT System data it needs to perform its functions.**

Those responsible for the TOE ensure that it is delivered, installed, managed, and operated in accordance with documented delivery and installation/setup procedures (OE.DELIVERY).

OE.DELIVERY satisfies this assumption.

A.DOMSEP **It is assumed that the IT environment will maintain a security domain for the Nortel VPN software that protects it from interference and tampering by untrusted subjects.**

The environment ensures that a security domain for the Nortel VPN Client software that protects it from interference and tampering by untrusted subjects is maintained (OE.DOMSEP).

OE.DOMSEP satisfies this assumption.

8.2 Security Functional Requirements Rationale

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

Table 12 - Relationship of Security Requirements to Objectives

Requirements	Objectives	O.I&A	O.AUDIT	O.SELFPROTECT	O.CONFIDENT	O.FUNCTIONS	O.ADMIN	O.INTEGRITY	O.REPLAY	O.FILTER	O.TEST	OE.TIME	OE.PROTECT	OE.NONBYPASS
TOE	FAU_GEN.1		✓											
	FAU_SAR.1		✓											
	FCS_CKM.1(a)			✓	✓			✓						
	FCS.CKM.4			✓	✓			✓						
	FCS_COP.1(a)			✓	✓			✓						
	FCS_COP.1(b)			✓	✓			✓						
	FCS_COP.1(d)			✓	✓			✓						
	FCS_COP.1(e)			✓	✓			✓						
	FCS_CKM.1(b)			✓	✓			✓						
	FDP_ACC.2	✓												
	FDP_ACF.1	✓												
	FDP_IFC.2(a)				✓			✓		✓				
	FDP_IFC.2(b)				✓			✓		✓				
	FDP_IFF.1(a)				✓			✓		✓				
	FDP_IFF.1(b)				✓			✓		✓				
	FDP_UCT.1				✓			✓		✓				
	FDP_UIT.1				✓			✓		✓				
	FIA_UAU.1	✓												
	FIA_UAU.5	✓												
	FIA_UID.2	✓												
	FMT_MOF.1(a)					✓	✓							
	FMT_MOF.1(b)					✓	✓							
	FMT_MSA.1(a)						✓							
	FMT_MSA.1(b)						✓							
	FMT_MSA.1(c)						✓							
	FMT_MSA.2					✓	✓							
	FMT_MSA.3(a)					✓	✓							
	FMT_MSA.3(b)					✓	✓							
	FMT_MSA.3(c)					✓	✓							
	FMT_SMF.1					✓	✓							
	FMT_SMR.1					✓	✓							

Objectives Requirements		O.I&A	O.AUDIT	O.SELFPROTECT	O.CONFIDENT	O.FUNCTIONS	O.ADMIN	O.INTEGRITY	O.REPLAY	O.FILTER	O.TEST	OE.TIME	OE.PROTECT	OE.NONBYPASS
	FPT_AMT.1										✓			
	FPT_RLT.1								✓					
	FPT_TST.1										✓			
	FTP_TRP.1					✓								
Env	FPT_RVM.1													✓
	FPT_SEP.1												✓	
	FPT_STM.1		✓									✓		✓

O.I&A **The TOE must be able to identify and authenticate users prior to allowing access to TOE functions and data.**

The TOE is required to enforce the Access Control SFP on subject and object by only allowing operations permitted by the Access Control SFP [FDP_ACC.2]. Prior to allowing an operation of subjects performed on an object, the TOE is required to check the authentication status and the privilege of the subject. Upon authentication, the TOE is required to provide

- The Primary Admin access to all the administrative functions.
- The Restricted Admin access to only authorized administrative functions while denying access to non authorized functions.
- The VPN User access to only the private network protected by the VPN while denying access to the administrative functions of the VPN.[FDP_ACF.1].

The TOE is required to allow to the user access to very limited functions prior to successfully authenticating and identifying themselves. Prior to accessing the functions of the TOE, users are required to successfully identify and authenticate themselves. The TOE is required to provide to users the following authentication mechanisms: username and password, RSA digital certificates. [FIA_UAU.1, FIA_UAU.5, and FIA_UID.2].

O.AUDIT **The TOE must record audit records for data accesses and use of the System functions.**

Security-relevant events must be defined and auditable for the TOE and all audit records will be associated with a user identity [FAU_GEN.1]. The TOE must provide the ability to review the audit trail of the System [FAU_SAR.1]. Time stamps associated with an audit record must be reliable [FPT_STM.1].

O.SELFPROTECT **The TOE must protect itself from unauthorized modifications and access to its functions and data.**

The TOE is required to use the specified algorithms to better protect itself. The RSA suite of algorithms and the Diffie-Hellman algorithm used by the TOE for cryptographic operations must be implemented according to RFC 3447 for RSA and RFC 2631 for Diffie-Hellman. The TOE is required to destroy unused keys by zeroizing them. For encryption and decryption operations, the TOE is required to use the 3DES and AES algorithms and they must be implemented according to FIPS 46-3 for 3DES and FIPS 197 for AES. For authentication, the TOE is required to use HMAC-SHA-1 and it must be implemented according to *RFC 2104.* For hashing, the TOE is required to use SHA-1 and it must be implemented according to *RFC 3174* [FCS_CKM.1(a), FCS_CKM.4, and FCS_COP.1(a,b,c,d,e,f)].

O.CONFIDENT The TOE must use the IPSec tunneling protocol to ensure confidentiality of data transmitted between the Nortel VPN Client and the Nortel VPN Router, and/or between two Nortel VPN Routers.

The TOE is required to use the specified tunneling protocol to better protect the confidentiality of the data transmitted between its different parts. The RSA suite of algorithms and the Diffie-Hellman algorithm used by the TOE for cryptographic operations must be implemented according to RFC 3447 for RSA and RFC 2631 for Diffie-Hellman. The TOE is required to destroy unused keys by zeroizing them. For encryption and decryption operations, the TOE is required to use the 3DES and AES algorithms and they must be implemented according to FIPS 46-3 for 3DES and FIPS 197 for AES. For authentication, the TOE is required to use HMAC-SHA-1 and it must be implemented according to *RFC 2104*. For hashing, the TOE is required to use SHA-1 and it must be implemented according to *RFC 3174* [FCS_CKM.1(a), FCS_CKM.4, and FCS_COP.1(a,b,d,c,e,f)].

All the operations between the different parts of the TOE must be scrutinized by the TOE against the VPN information flow control SFP and the Firewall information flow control SFP using specific security attributes. During this task, the TOE is required to make use of its Firewall, NAT, and IPSec tunneling protocol implementations [FDP_IFC.2(a), FDP_IFF.1(a), FDP_UCT.1, and FDP_UIT.1].

O.FUNCTIONS The TOE must provide functionality that enables only authorized user to establish VPN sessions with the TOE using IPSec protocol.

Using the Access Control SFP, the TSF is required to provide the ability to restrict managing the behavior, and modifying the security attributes of functions of the TOE to authorized users of the TOE [FMT_MOF.1(a,b)]. The TOE is required to only accept secure values for security attributes [FMT_MSA.2]. The TOE SFPs are required to provide restrictive default values and to alternatively provide authorized users the ability to override default values for security attributes that are used to enforce the SFP [FMT_MSA.3(a,b,c)].

The TSF is required to perform security management functions such as create log-ins and assign roles to user log-in IDs [FMT_SMF.1]. The TOE must be able to recognize the different administrative and user roles that exist for the TOE [FMT_SMR.1].

The TSF is required to provide a logically distinct and protected communication path for secure VPN communication with remote users [FTP_TRP.1].

O.ADMIN The TOE will provide facilities to enable an authorized administrator to effectively manage the TOE and its security function, and will ensure that only authorized administrators are able to access such functionality.

The TSF is required to provide the ability to restrict managing the behavior, and modifying the security attributes of functions of the TOE to authorized users of the TOE [FMT_MOF.1(a,b)].

The TSF is required to enforce the *Access Control SFP* to restrict the ability to *modify* the security attributes to authorized administrators [FMT_MSA.1(a,b,c,d,e)].

The TOE is required to only accept secure values for security attributes [FMT_MSA.2]. The TOE SFPs are required to provide restrictive default values and to alternatively provide authorized users the ability to override default values for security attributes that are used to enforce the SFP [FMT_MSA.3(a,b,c)].

The TSF is required to perform security management functions such as create users and assign roles to users [FMT_SMF.1]. The TOE must be able to recognize the different administrative and user roles that exist for the TOE [FMT_SMR.1].

O.INTEGRITY The TOE must use the IPSec tunneling protocol to ensure integrity of data transmitted between the Nortel VPN Client and the Nortel VPN Router, and/or between two Nortel VPN Routers.

The TSF is required to enforce the *information flow control SFP* on connections and all operations that cause information to flow to and from subjects covered by the SFP [FDP_IFC.2(a,b)].

The TSF is required to enforce the *information flow control SFP* based the types of subject and information security attributes. The TSF is required to permit information flow between a controlled subject and controlled information via a controlled operation if the connection is allowed. The TSF is required to deny an information flow based on the packet sequence number [FDP_IFF.1(a,b)].

The TSF is required to enforce the *information flow control SFP* in order to send or receive objects in a manner protected from unauthorised disclosure [FDP_UCT.1].

The TSF is required to enforce the *information flow control SFP* in order to send or receive user data in a manner protected from errors, and to determine whether an error has occurred [FDP_UIT.1].

The TOE is required to use the specified tunneling protocol to better protect the integrity of the data transmitted in between its different parts. The RSA suite of algorithms and the Diffie-Hellman algorithm used by the TOE for cryptographic operations must be implemented according to RFC 3447 for RSA and RFC 2631 for Diffie-Hellman. The TOE is required to destroy unused keys by zeroizing them. For encryption and decryption operations, the TOE is required to use the 3DES and AES algorithms and they must be implemented according to FIPS 46-3 for 3DES and FIPS 197 for AES. For authentication, the TOE is required to use HMAC-SHA-1 and it must be implemented according to *RFC 2104.* For hashing, the TOE is required to use SHA-1 and it must be implemented according to *RFC 3174* [FCS_CKM.1(a), FCS_CKM.4, and FCS_COP.1(a,b,c,d,e,f)].

O.REPLAY The TOE must provide functionality that enables detection of replay attack and take appropriate action if an attack is detected.

The TOE is required to detect replay attacks on established IPSec sessions; if a replay attack is detected, the TOE is TOE is required to drop packets from the attacker [FPT_RLT.1].

O.FILTER The TOE must filter all incoming and outgoing packets that pass through it, and accept or reject packets based on their attributes.

All operations between the different parts of the TOE must be scrutinized by the TOE against the VPN information flow control SFP and the Firewall information flow control SFP using specific security attributes. During this task, the TOE is required to make use of its Firewall, NAT, and IPSec tunneling protocol implementations [FDP_IFC.2(a,b), FDP_IFF.1(a,b), FDP_UCT.1, and FDP_UIT.1].

O.TEST The TOE must provide functionality that enables testing of its correct functioning and integrity.

During start-up and periodically during normal operation, the TOE is required to run a suite of self tests to demonstrate the correct operation of the TSF. The TOE is also required to provide authorized users with the ability to verify the integrity of TSF Data and TSF executable code [FPT_AMT.1 and FPT_TST.1].

OE.TIME **The environment must provide reliable timestamps for the time-stamping of audit events.**

Time stamps associated with an audit record must be reliable [FPT_STM.1].

OE.PROTECT **The environment must protect the TOE from interference and tampering by untrusted subjects.**

The IT Environment must protect the TOE from intentional attacks and unintentional interference [FPT_SEP.1].

OE.NONBYPASS **The environment must ensure that TSP enforcement functions are invoked and succeed before each function within the TSC is allowed to proceed.**

The IT Environment must ensure that the TOE receives reliable time information for time stamps from the Environment [FPT_RVM.1], and only receives it from an authorized and reliable source [FPT_STM.1].

8.3 Security Assurance Requirements Rationale

EAL 4+ was chosen to provide a basic level of independently assured security and thorough investigation of the TOE and its development. 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 TOE may operate in a hostile environment, it is expected to be protected by other products and processes designed to address threats that correspond with the intended environment. At EAL 4+, the TOE will have incurred an independent vulnerability analysis to support its introduction into the hostile environment.

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

8.4 Rationale for Strength of Function

The TOE minimum strength of function is SOF-basic. The evaluated TOE is intended to operate in commercial and DoD low robustness environments processing unclassified information. This security function is consistent with the security objectives described in Section 4.

8.5 Dependency Rationale

This ST satisfies all the requirement dependencies of the CC. Table 13 lists each requirement to which the TOE claims conformance with a dependency and indicates whether the dependent requirement was included. As indicated by the table, all dependencies have been met.

Table 13 - Functional Requirements Dependencies

SFR ID	Dependencies	Dependency Met
FAU_GEN.1	FPT_STM.1	✓
FAU_SAR.1	FAU_GEN.1	✓
FCS_CKM.1(a)	FCS_COP.1 FCS_CKM.4 FMT_MSA.2	✓

SFR ID	Dependencies	Dependency Met
FCS.CKM.4	FCS_CKM.1(a) FMT_MSA.2	✓
FCS_COP.1	FCS_CKM.1(a) FCS_CKM.4 FMT_MSA.2	✓
FDP_ACC.2	FDP_ACF.1	✓
FDP_ACF.1	FDP_ACC.1[9] FMT_MSA.3	✓
FDP_IFC.2	FDP_IFF.1	✓
FDP_IFF.1	FDP_IFC.1[10]	✓
FDP_UCT.1	FTP_TRP.1 FDP_ACC.1[9] / FDP_IFC.1[10]	✓
FDP_UIT.1	FDP_ACC.1[9] / FDP_IFC.1[10] FTP_TRP.1	✓
FIA_UAU.1	FIA_UID.1[11]	✓
FIA_UAU.5	[none]	✓
FIA_UID.2	[none]	✓
FMT_MOF.1	FMT_SMF.1 FMT_SMR.1	✓
FMT_MSA.1	FDP_ACC.1[9] / FDP_IFC.1[10] FMT_SMF.1 FMT_SMR.1	✓
FMT_MSA.2	ADV_SPM.1 FDP_ACC.1[9] / FDP_IFC.1[10] FMT_MSA.1 FMT_SMR.1	✓
FMT_MSA.3	FMT_MSA.1 FMT_SMR.1	✓
FMT_SMF.1	[none]	✓
FMT_SMR.1	FIA_UID.1[11]	✓
FPT_AMT.1	[none]	✓
FPT_RPL.1	[none]	✓

[9] Met by hierarchical SFR: FDP_ACC.2
[10] Met by hierarchical SFR: FDP_IFC.2
[11] Met by hierarchical SFR: FIA_UID.2

SFR ID	Dependencies	Dependency Met
FPT_TST.1	FPT_AMT.1	✓
FTP_TRP.1	[none]	✓

8.6 TOE Summary Specification Rationale

8.6.1 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 a set of requirements with rationale that indicates how these requirements are satisfied by aspects of the corresponding security function. The set of security functions work together to satisfy all of the security 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. Please see Section 6 - TOE Summary Specification for more details.

Table 14 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. Refer to Section 8.7 for Strength of Function.

Table 14 - Mapping of Security Functional Requirements to TOE Security Functions

TOE Security Function	SFR
Security Audit	FAU_GEN.1 FAU_SAR.1
Cryptographic Support	FCS_CKM.1(a) FCS.CKM.4 FCS_COP.1
User Data Protection	FDP_ACC.2 FDP_ACF.1 FDP_IFC.2 FDP_IFF.1 FDP_UCT.1 FDP_UIT.1
Identification and Authentication	FIA_UAU.1 FIA_UAU.5 FIA_UID.2
Security Management	FMT_MOF.1 FMT_MSA.1 FMT_MSA.2 FMT_MSA.3 FMT_SMF.1 FMT_SMR.1
Protection of the TSF	FPT_AMT.1 FPT_RPL.1 FPT_TST.1
Trusted Path/Channels	FTP_TRP.1

8.6.2 TOE Summary Specification Rationale for the Security Assurance Requirements

8.6.2.1 Configuration Management

The Configuration Management documentation provides a description of tools used to control the configuration items and how they are used by Nortel. The documentation provides a complete configuration item list and a unique reference for each item. Additionally, the configuration management system is described including procedures that are used by developers to control and track changes that are made to the TOE. The documentation further details the TOE configuration items that are controlled by the configuration management system.

Corresponding CC Assurance Components:

- Configuration Items

8.6.2.2 Secure Delivery and Operation

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

Corresponding CC Assurance Components:

- Delivery Procedures
- Installation, Generation, and Start-Up Procedures

8.6.2.3 Development

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

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

Corresponding CC Assurance Components:

- Functional Specification with Complete Summary
- Security-Enforcing High-Level Design
- Descriptive Low-Level Design
- Implementation of the TSF
- Informal TOE Security Policy Model
- Informal Representation Correspondence

8.6.2.4 Guidance Documentation

The Nortel Guidance documentation provides administrator and user guidance on how to securely operate the TOE. The Administrator Guidance provides descriptions of the security functions provided by the TOE. Additionally, it provides detailed accurate information on how to administer the TOE in a secure manner and how to effectively use the TSF privileges and protective functions. The User Guidance provided directs users on how to operate the TOE in a secure manner. Additionally, User Guidance explains the user-visible security functions and how they are to be used and explains the user's role in maintaining the TOE's Security. Nortel provides single versions of documents which address the administrator Guidance and User Guidance; there are no separate guidance documents specifically for non-administrator users of the TOE.

Corresponding CC Assurance Components:

- Administrator Guidance
- User Guidance

8.6.2.5 Life Cycle Support Documents

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

Corresponding CC Assurance Components:

- Identification of Development Security Measures
- Flaw Reporting Procedures
- Developer Defined Life Cycle Model
- Well-defined Development Tools

8.6.2.6 Tests

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

Corresponding CC Assurance Components:

- Analysis of Coverage
- High-Level Design
- Functional Testing
- Independent Testing

8.6.2.7 Vulnerability and TOE Strength of Function Analyses

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

Corresponding CC Assurance Components:

- Validation of Analysis
- Strength of TOE Security Function Evaluation
- Independent Vulnerability Analysis

8.7 Strength of Function

A Strength of Function rating of “SOF-basic” is claimed for this TOE to meet the EAL 4+ assurance requirements. This SOF is sufficient to resist the threats identified in Section 3. Section 4 provides evidence that demonstrates that TOE threats are countered by the TOE security objectives. Section 8 demonstrates that the security objectives for the TOE and the TOE environment are satisfied by the security requirements. The evaluated TOE is intended to operate in commercial and DoD 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 functions and security functional requirements which have probabilistic or permutational functions are FIA_UAU.1, and FIA_UAU.5.

9 Acronyms

Table 15 - Acronyms

Acronym	Definition
3DES	Triple DES
AES	Advanced Encryption Standard
CC	Common Criteria
CLI	Command Line Interface
CPU	Central Processing Unit
DES	Data Encryption Standard
DoD	Department of Defense
EAL	Evaluation Assurance Level
FIPS	Federal Information Processing Standard
GUI	Graphical User Interface
HMAC	Hashed Message Authentication Code
ICMP	Internet Control Message Protocol
ID	Identification / Identifier
IFC	Information Flow Control
IP	Internet Protocol
IPSec	IP Security
IT	Information Technology
KAT	Known Answer Test
L2F	Layer Two Forwarding
L2TP	Layer Two Tunneling Protocol
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
NAT	Network Address Translation
OS	Operating System
OSI	International Organization for Standardization
PC	Personal Computer
PP	Protection Profile
PPTP	Point-Point Tunneling Protocol
RADIUS	Remote Authentication Dial-In User Server/Service
RNG	Random Number Generator
RSA	Rivest, Shamir, & Adleman
SAR	Security Assurance Requirement
SFP	Security Functional Policy
SFR	Security Functional Requirement

Acronym	Definition
SHA	Secure Hash Algorithm
SOF	Strength of Function
ST	Security Target
TCP	Transmission Control Protocol
TOE	Target of Evaluation
TSF	TOE Security Function
TSP	TOE Security Policy
UDP	User Datagram Protocol
VPN	Virtual Private Network
WAN	Wide Area Network