totalsecurity™

Check Point SOFTWARE TECHNOLOGIES LTD.

Check Point VPN-1 Power/UTM NGX R65

Security Target

Version 1.0

March 4, 2009

Prepared for:

Check Point SOFTWARE TECHNOLOGIES LTD.

5 Ha'Solelim St.

Tel Aviv, Israel 67897

Prepared by:

Metatron Security Services

Metatron Security Services Ltd.

66 Yosef St.,

Modiin, Israel 71724

Document Version Control Log

Version	Date	Author	Description
Version 0.1	September 4, 2007	Nir Naaman	Extracted from NGX R60 ST. Added SSL VPN, OCSP, support for Marvell chipsets.
Version 0.3	November 1, 2007	Nir Naaman	Added SecureClient Mobile support.
Version 0.5	August 11, 2008	Nir Naaman	Changed TOE identification to NGX R65 with HFA 30, including both Open Server and Check Point appliance versions. Added reference to SmartConsole HFA 01. Added Windows Vista to the list of supported platforms for SmartConsole Updated list of supported appliances.
Version 1.0	March 4, 2009	Nir Naaman	EAL4+ALC_FLR.3 ST approved for public release.

Table of Contents

List of Tables

List of Figures

1. Introduction

1.1. ST Identification

Title: Check Point VPN-1 Power/UTM NGX R65 Security Target

ST Version: 1.0

ST Date: March 4, 2009

Author: Nir Naaman

TOE Software Identification:

Check Point VPN-1 Power/UTM NGX R65 with HFA 30[1]

TOE Hardware/Operating System Identification:

The TOE consists of TOE security policy enforcement software running on any of the appliance platforms and operating system combinations listed in Appendix A - TOE Hardware Platforms. This includes the following classes of appliances:

- Check Point Power-1 and UTM-1 security appliances
- Open Servers supporting the Check Point SecurePlatform operating system
- Nokia Firewall/VPN appliances

TOE management software is always installed on a separate platform running the Check Point SecurePlatform operating system, selected from the list given in Section A.1. The platform selected for this purpose is not used for TOE identification.

TOE software also includes a Management GUI product (SmartConsole) that is installed on a standard PC (outside the TOE) running a Microsoft Windows operating system. The evaluated version is: SmartConsole NGX R65 with HFA 01.

TOE Support Program Identification: Enterprise Software Subscription[2]

CC Version: Common Criteria for Information Technology Security Evaluation, Version 2.2 Revision 256, January 2004, CCIMB-2004-01-001

Evaluation Assurance Level (EAL):

EAL 4, augmented with ALC_FLR.3 (systematic flaw remediation).

[1] The TOE software identification is a combination of the product name (Check Point VPN-1 Power/UTM), the product version (NGX R65), and a Hot Fix Accumulator (HFA) number. This combination uniquely identifies a software build for each of the supported appliance classes. Throughout this document, the product is referred to as Check Point VPN-1 Power/UTM, omitting the HFA number identified here.

[2] Enterprise Software Subscription is required for receiving software upgrades, as part of Check Point's flaw remediation procedures. Note that Enterprise Software Subscription is a prerequisite to purchasing all Check Point Enterprise Support Programs.

Keywords: Information flow control, firewall, proxy server, traffic filter, VPN, TLS, IPSec, IDS/IPS, intrusion detection, Medium Robustness Environments

1.2. ST Overview

Check Point VPN-1 Power/UTM is a network perimeter security device that provides controlled connectivity between two or more network environments. It mediates information flows between clients and servers located on internal and external networks governed by the firewall.

The product provides a broad set of information flow controls, including traffic filtering, application-level proxies and intrusion detection and prevention capabilities. IPSec and SSL VPN functionality encrypts and authenticates network traffic to and from selected peers, in order to protect the traffic from disclosure or modification over untrusted networks.

Management can be performed either locally or remotely using management interfaces that are included in the Target of Evaluation (TOE).

Check Point VPN-1 Power/UTM meets and exceeds[3] the functional requirements of two U.S. DoD Medium Robustness Protection Profiles, for proxy and traffic filtering firewalls, respectively. These PPs require the product to provide appropriate security to process unclassified or sensitive but unclassified information in the Mission-Critical Categories. Mission-Critical Categories refer to DoD systems that handle information vital to the operational readiness or mission effectiveness of deployed and contingency forces in terms of both content and timeliness.

In addition, the product meets the requirements of the NSA System Protection Profile for an Intrusion Detection System (IDSSPP). The IDSSPP provides for a level of protection which is appropriate for IT environments that require detection of malicious and inadvertent attempts to gain inappropriate access to IT resources.

The evaluation assurance level claimed in this Security Target was augmented in relationship to the assurance requirements specified in the claimed PPs in order to provide additional assurance that the TOE is resistant to attacks performed by attackers possessing a moderate (greater than low) attack potential.

[3] Because the AVA_VLA.3 evaluation revalidation had not completed at the time of the publication of this Security Target, this Security Target does **not** claim conformance to the two medium robustness protection profiles identified here.

1.3. Conformance Claims

1.3.1. CC Conformance

The TOE is conformant with the following CC specifications:

- Common Criteria for Information Technology Security Evaluation Part 2: Security functional requirements, Version 2.2, January 2004, CCIMB-2004-01-002, extended (Part 2 Extended)
- Common Criteria for Information Technology Security Evaluation Part 3: Security assurance requirements, Version 2.2 Revision 256, January 2004, CCIMB-2004-01-003, conformant (Part 3 Conformant)

1.3.2. Assurance Package Conformance

The TOE is conformant with the following CC specifications:

- Evaluation Assurance Level (EAL) 4 augmented with ALC_FLR.3.

1.3.3. PP Conformance

The TOE is Protection Profile Conformant with the following Protection Profiles:

- Intrusion Detection System System Protection Profile, Version 1.6, April 4, 2006

The TOE meets all of the security requirements of the following Protection Profiles, except for AVA_VLA.3[4]:

- U.S. Department of Defense Application-Level Firewall Protection Profile for Medium Robustness Environments, Version 1.0, June 2000
- U.S. Department of Defense Traffic-Filter Firewall Protection Profile for Medium Robustness Environments, Version 1.4, May 1, 2000

[4] Because the AVA_VLA.3 evaluation had not completed at the time of the publication of this Security Target, this Security Target does **not** claim conformance to the two medium robustness protection profiles identified here.

1.4. Document Organization

Section 1 provides the introductory material for the security target.

Section 2 is the TOE description.

Section 3 describes the expected environment for the TOE. This section also defines the set of threats that are to be addressed by either the technical countermeasures implemented in the TOE or through environmental controls.

Section 4 defines the security objectives for both the TOE and the TOE environment.

Section 5 gives the functional and assurance requirements derived from the Common Criteria, Parts 2 and 3, respectively that must be satisfied by the TOE.

Section 6 describes the security functions and assurance measures provided by the TOE that address the security requirements. In addition, it identifies the method used to determine compliance with cryptographic standards[5].

Section 7 is the Protection Profile claims statement. The PP claims statement describes any tailoring or additions made on top of the claimed PPs.

Section 8 provides a rationale that traces through the levels of abstraction given in the ST (environment, requirements, objectives, and TSS) in order to demonstrate that the ST is a complete and cohesive set of requirements, providing an effective set of IT security countermeasures within the security environment, and that the TOE summary specification addresses the stated requirements. The rationale also demonstrates that the PP conformance claim is valid.

[5] Identification of Standards compliance determination per guidance given in [I-0427].

1.5. References

The following external documents are referenced in this Security Target.

Identifier	Document
[802.1Q]	Virtual Bridged Local Area Networks, IEEE Std 802.1Q, 2003 Edition, May 2003
[APP-PP]	U.S. Department of Defense Application-level Firewall Protection Profile for Medium Robustness Environments, Version 1, June 28, 2000
[CAPP]	Controlled Access Protection Profile, Version 1.d, October 8, 1999
[CC]	Common Criteria for Information Technology Security Evaluation Parts 1-3, Version 2.2 Revision 256, January 2004, CCIMB-2004-01-001, 002 and 003
[CEM]	Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, Version 2.2 Revision 256, January 2004, CCIMB-2004-01-004
[FIPS46-3]	NIST FIPS PUB 46-3 – Specifications for the Data Encryption Standard (DES), October 25, 1999
[FIPS140]	NIST FIPS PUB 140–2, Security Requirements for Cryptographic Modules, December 3, 2002
[FIPS197]	NIST FIPS PUB 197 – Specification for the Advanced Encryption Standard (AES), November 26, 2001
[FIPS198]	NIST FIPS PUB 198 – Keyed-Hash Message Authentication Code (HMAC), March 6, 2002
[FIPSPOL]	*VPN-1 FIPS 140-2 Non-Proprietary Security Policy*, Version 1.0, October 2006
[I-0388]	NIAP Interpretation I-0388: What Is The Difference Between "Sort" and "Order"?
[I-0410]	NIAP Interpretation I-0410: Auditing Of Subject Identity For Unsuccessful Logins
[I-0422]	NIAP Interpretation I-0422: Clarification of "Audit Records"
[I-0427]	NIAP Interpretation I-0427: Identification of Standards
[IDSSPP]	Intrusion Detection System System Protection Profile, Version 1.6, April 4, 2006
[LDAP]	RFC 1777 - Lightweight Directory Access Protocol, March 1995
[PD-0018]	NIAP Precedent Decision PD-0018: Usage of the Term "Loopback Network" in the Application Level Firewall PP
[PD-0026]	NIAP Precedent Decision PD-0026: Typographical error in the ALFWPP-MED with respect to FDP_IFF.1(1) and FDP_IFF.1(2)
[PD-0055]	NIAP Precedent Decision PD-0055: Effect of Addition of Environmental Assumptions on PP Compliance
[PD-0071]	NIAP Precedent Decision PD-0071: Identification of Operations on Security Functional Requirements
[PD-0086]	NIAP Precedent Decision PD-0086: What SOF Claim is appropriate when there are no probabilistic or permutational mechanisms

[PD-0087] NIAP Precedent Decision PD-0087: STs Adding Requirements to Protection Profiles

[PD-0097] Compliance with IDS System PP Export Requirements

[PD-0105] NIAP Precedent Decision PD-0105: Acceptability of IKE Authentication as "Single Use" In Firewall PPs

[PD-0113] NIAP Precedent Decision PD-0113: Use of Third-Party Security Mechanisms in TOE Evaluations

[PD-0115] NIAP Precedent Decision PD-0115: Third Party Authentication is permitted by the ALFWPP-MR

[RFC0854] RFC 0854 – TELNET Protocol Specification, May 1983

[RFC0959] RFC 0959 – File Transfer Protocol (FTP), October 1985

[RFC1305] RFC 1305 – Network Time Protocol (Version 3) – Specification, Implementation and Analysis, March 1992

[RFC1777] RFC 1777 – Lightweight Directory Access Protocol, March 1995

[RFC1778] RFC 1778 - The String Representation of Standard Attribute Syntaxes, March 1995

[RFC2104] RFC 2104 – HMAC: Keyed-Hashing for Message Authentication, February 1997

[RFC2138] RFC 2138 – Remote Authentication Dial In User Service (RADIUS), April 1997

[RFC2246] RFC 2246 – The TLS Protocol Version 1.0, January 1999

[RFC2401] RFC 2401 – Security Architecture for the Internet Protocol, November 1998

[RFC2404] RFC 2404 – The Use of HMAC-SHA-1-96 within ESP and AH, November 1998

[RFC2406] RFC 2406 – Encapsulating Security Payload (ESP), November 1998

[RFC2409] RFC 2409 - The Internet Key Exchange (IKE), November 1998

[RFC2616] RFC 2616 – Hypertext Transfer Protocol – HTTP/1.1, June 1999

[RFC2818] RFC 2818 – HTTP over TLS, May 2000

[RFC2821] RFC 2821 – Simple Mail Transfer Protocol, April 2001

[RFC2865] RFC 2865 – Remote Authentication Dial In User Service (RADIUS), June 2000

[RFC3947] RFC 3947 – Negotiation of NAT-Traversal in the IKE, January 2005

[RFC3948] RFC 3948 – UDP Encapsulation of IPsec ESP Packets, January 2005

[RI#137] Final Interpretation for RI # 137 – Rules governing binding should be specifiable, CCIMB, January 30, 2004

[TFF-PP] U.S. Department of Defense Traffic-Filter Firewall Protection Profile for Medium Robustness Environments, Version 1.4, May 1, 2000

1.6. Conventions

The notation, formatting, and conventions used in this Security Target (ST) are consistent with version 2.2 of the Common Criteria for Information Technology Security Evaluation. Font style and clarifying information conventions were developed to aid the reader.

1.6.1. Security Environment Considerations and Objectives

The naming convention for security environment considerations and for objectives is as follows:

- Assumptions are denoted by the prefix “A.”, e.g. “A.PHYSEC”.
- Organizational Security Policy statements are denoted by the prefix “P.”, e.g. “P.CRYPTO”.
- Threats are denoted by the prefix “T.”, e.g. “T.NOAUTH”.
- Objectives for the IT TOE are denoted by the prefix “O.”, e.g. “O.IDAUTH”.
- Objectives for the IT environment are denoted by the prefix “OE.”, e.g. “OE.VPN”.
- Objectives for the non-IT environment are denoted by the prefix “NOE.”, e.g. “NOE.PHYSEC”.

1.6.2. Security Functional Requirements

The CC permits four functional and assurance requirement component operations: assignment, iteration, refinement, and selection. These operations are defined in the Common Criteria, Part 1, paragraph 4.4.1 as:

- Iteration: allows a component to be used more than once with varying operations;
- Assignment: allows the specification of parameters;
- Selection: allows the specification of one or more items from a list; and
- Refinement: allows the addition of details.

1.6.2.1. Iteration

Where necessary to cover different aspects of the same requirement (e.g. identification of more than one type of user), repetitive use of the same component to cover each aspect is permitted. Iteration is used together with assignment, selection, and refinement in order to specify the different iterations. In this document, iterations are identified with a number inside parentheses ("(#)"). These follow the short family name and allow components to be used more than once with varying operations.

Security functional requirements for the IT environment are identified by an iteration identifier of the form "(Env)".

1.6.2.2. Assignment

Some components have elements that contain parameters that enable the ST author to specify a set of values for incorporation into the ST to meet a security objective. These elements clearly identify each parameter and constraint on values that may be assigned to that parameter. Any aspect of an element whose acceptable values can be unambiguously described or enumerated can be represented by a parameter. The parameter may be an attribute or rule that narrows the requirement to a specific value or range of values. For instance, based on a security objective, an element within a component may state that a given operation should be performed a number of times. In this case, the assignment would provide the number, or range of numbers, to be used in the parameter.

1.6.2.3. Selection

This is the operation of picking one or more items from a list in order to narrow the scope of an element within a component.

1.6.2.4. Refinement

For all components, the ST author is permitted to limit the set of acceptable implementations by specifying additional detail in order to meet a security objective. Refinement of an element within a component consists of adding these technical details. In order for a change to a component to be considered a valid refinement, the change must satisfy all the following conditions:

- A TOE meeting the refined requirement would also meet the original requirement, as interpreted in the context of the ST;
- In cases where a refined requirement is iterated, it is permissible that each iteration address only a subset of the scope of the requirement; however, the sum of the iterations must together meet the entire scope of the original requirement;
- The refined requirement does not extend the scope of the original requirement; and
- The refined requirement does not alter the list of dependences of the original requirement.

1.6.3. Other Notations

1.6.3.1. Extended Requirements

Extended requirements are additional functional requirements defined in this ST that are not contained in Part 2 and/or additional assurance requirements not contained in Part 3. These requirements are used when security functionality is provided by the TOE that cannot be described by Part 2 or Part 3 requirements. A rationale for the usage of such extended requirements is given in section 8.2.4. Extended requirements receive names similar to existing Part 2 and Part 3 components, with an additional suffix of (EXP) which is appended to the component's short name.

1.6.3.2. Application Notes

Application Notes are used to clarify the author's intent for a given requirement. These are italicized (except where taken directly from a claimed PP) and will appear following the component needing clarification.

1.6.3.3. Footnotes

Footnotes[6] are used to provide further clarification for a statement, without breaking the flow of the text.

1.6.3.4. References

References to other documents are given using a short name in square brackets, e.g. "[PD-0105]". The identification of the referenced document is provided in Section 1.5.

[6] This is an example of a footnote.

1.6.4. Highlighting Conventions

The conventions for SFRs described above in sections 1.6.2 and 1.6.3 are expressed in chapter 5 by using combinations of bolded, italicized, and underlined text as specified in Table 1-1 below.

These conventions are applied in respect to requirements derived from the firewall PPs, which are the primary PPs for this ST. Assignments, selections, and refinements that were already performed in the firewall PPs or IDS System PP are not identified via a highlighting convention in this ST. This is consistent with the guidance given in [PD-0071]. Where a requirement appears in both the firewall PPs and the IDS System PP, the operations performed on the requirement component in relation to the IDS System PP are not identified using a highlighting convention, to avoid confusion with the firewall PPs; these operations are listed in column 5 of Table 5-1.

Table 1-1- SFR Highlighting Conventions

Convention	Purpose	Operation
Boldface	Boldface text denotes completed component assignments. Example: *5.1.2.5 Cryptographic operation (FCS_COP.1(3))* FCS_COP.1.1(3) The TSF shall perform **encryption and decryption of VPN traffic** in accordance with a specified cryptographic algorithm: …	(completed) Assignment
<u>Underline</u>	Underlined text denotes completed component selections (out of a set of selection options provided in the original CC requirement). Example: *5.1.6.1 Abstract machine testing (FPT_AMT.1)* FPT_AMT.1.1 The TSF shall run a suite of tests <u>during initial start-up</u> to demonstrate the correct operation of the security assumptions provided by the abstract machine that underlies the TSF.	(completed) Selection
<u>Boldface Underline</u>	Underlined boldface text highlights component refinements. This includes refinement of an operation that was completed in the PP. Example: *5.1.5.11. Static attribute initialization (FMT_MSA.3)* FMT_MSA.3.1 The TSF shall enforce the UNAUTHENTICATED SFP**<u>, TRAFFIC FILTER SFP</u>** and AUTHENTICATED SFP to provide restrictive default values for information flow security attributes that are used to enforce the SFP.	Refinement

Convention	Purpose	Operation
Parentheses (iteration #)	Parentheses and an iteration number inform the reader that the requirement component will be used multiple times. Examples: *5.1.5.6. Management of security attributes (FMT_MSA.1(1))* FMT_MSA.1.1(1) The TSF shall enforce the UNAUTHENTICATED SFP and TRAFFIC FILTER SFP to restrict … *5.1.5.7 Management of security attributes (FMT_MSA.1(2))* FMT_MSA.1.1(2) The TSF shall enforce the AUTHENTICATED SFP to restrict …	Iteration 1 (FMT_MSA.1) Iteration 2 (FMT_MSA.1)
	5.3.1.1 Multiple authentication mechanisms (FIA_UAU.5(Env)) FIA_UAU.5.1(Env) The IT Environment shall…	SFR for the IT environment (FIA_UAU.5)
Italics	Italics are used for application notes. Example: Application Note: *All users, whether authenticated or not, will always be identified at least by a source network identifier*.	Application Note
Extended Requirement (EXP)	The suffix "(EXP)" denotes an extended requirement that was not taken from Part 2 or Part 3 of the CC, but was explicitly defined specifically to provide security functionality that is relevant to this ST. Examples: *5.1.8.3. Analyzer react (IDS_RCT(EXP).1)* IDS_RCT(EXP).1.1 The System shall send an alarm…	Extended Requirement

1.7. Terminology

In the Common Criteria, many terms are defined in Section 2.3 of Part 1. The following sections are a refined subset of those definitions, listed here to aid the user of this ST. The glossary is augmented with terms that are specific to the Check Point VPN-1 Power/UTM product.

1.7.1. Glossary

Access Interaction between an entity and an object that results in the flow or modification of data.

Access Control Security service that controls the use of resources[7] and the disclosure and modification of data.[8]

Accountability Property that allows activities in an IT system to be traced to the entity responsible for the activity.

Administrator A user who has been specifically granted the authority to manage some portion or all of the TOE and whose actions may affect the TSP. Administrators may possess special privileges that provide capabilities to override portions of the TSP.

Assurance A measure of confidence that the security features of an IT system are sufficient to enforce its security policy.

Asymmetric Cryptographic System

A system involving two related transformations; one determined by a public key (the public transformation),and another determined by a private key (the private transformation) with the property that it is computationally infeasible to determine the private transformation (or the private key) from knowledge of the public transformation (and the public key).

Asymmetric Key The corresponding public/private key pair needed to determine the behaviour of the public/private transformations that comprise an asymmetric cryptographic system.

Attack An intentional act attempting to violate the security policy of an IT system.

Authentication Security measure that verifies a claimed identity.

Authentication data Information used to verify a claimed identity.

Authorisation Permission, granted by an entity authorised to do so, to perform functions and access data.

[7] Hardware and software.

[8] Stored or communicated.

Authorised user	An authenticated user who may, in accordance with the TSP, perform an operation.
Availability	Timely[9], reliable access to IT resources.
Compromise	Violation of a security policy.
Confidentiality	A security policy pertaining to disclosure of data.
Cryptographic key (key)	A parameter used in conjunction with a cryptographic algorithm that determines: • the transformation of plaintext data into cipher text data, • the transformation of cipher text data into plaintext data, • a digital signature computed from data, • the verification of a digital signature computed from data, or • a digital authentication code computed from data.
Entity	A subject, object, user, or another IT device, which interacts with TOE objects, data, or resources.
External IT entity	Any trusted Information Technology (IT) product or system, outside of the TOE, which may, in accordance with the TSP, perform an operation.
Identity	A representation (e.g., a string) uniquely identifying an authorised user, which can either be the full or abbreviated name of that user or a pseudonym.
INSPECT	A patented Check Point virtual machine for stateful inspection.
Integrity	A security policy pertaining to the corruption of data and TSF mechanisms.
IPSec VPN	A Virtual Private Network implementation based on the IKE/IPSec protocols.
Named Object	An object that exhibits all of the following characteristics: • The object may be used to transfer information between subjects of differing user identities within the TSF. • Subjects in the TOE must be able to request a specific instance of the object. • The name used to refer to a specific instance of the object must exist in a context that potentially allows subjects with

[9] According to a defined metric.

different user identities to request the same instance of the object.

Non-Repudiation A security policy pertaining to providing one or more of the following:

- To the sender of data, proof of delivery to the intended recipient,
- To the recipient of data, proof of the identity of the user who sent the data.

Object An entity that contains or receives information and upon which subjects perform operations.

Operational Environment

The total environment in which a TOE operates. It includes the physical facility and any physical, procedural, administrative and personnel controls.

OPSEC API An application programming interface published by the OPSEC alliance program.

Peer TOEs Mutually authenticated TOEs that interact to enforce a common security policy.

Secure Internal Communications

Protection for management traffic using the TLS protocol.

Security attributes TSF data associated with subjects, objects, and users that is used for the enforcement of the TSP.

Stateful Inspection A Check Point technology for performing security analysis of network traffic at the network layer, and performing information flow control based on any part of the data being mediated, as well as on state information.

SmartCenter A Check Point management server product.

SmartDashboard The management GUI for SmartCenter Server

SmartDefense A unified security framework for various components that identify and prevent attacks.

SmartDefense Update

The capability to load IDS/IPS attack signature updates.

SmartView Tracker A counterpart to SmartDashboard, for reviewing audit trails.

SmartView Monitor A counterpart to SmartDashboard, for viewing TOE status.

SSL VPN A Virtual Private Network implementation based on the TLS protocol.

Subject An entity within the TSC that causes operations to be performed.

Symmetric key	A single, secret key used for both encryption and decryption in symmetric cryptographic algorithms.
Threat	Capabilities, intentions and attack methods of adversaries, or any circumstance or event, with the potential to violate the TOE security policy.
Threat Agent	Any human user or Information Technology (IT) product or system, which may attempt to violate the TSP and perform an unauthorised operation with the TOE.
User	Any entity (human user or external IT entity) outside the TOE that interacts with the TOE.
Vulnerability	A weakness that can be exploited to violate the TOE security policy.

1.7.2. Abbreviations

Abbreviation	Description
AES	Advanced Encryption Standard
API	Application Programming Interface
CA	Certificate Authority
CC	Common Criteria
CCIMB	Common Criteria International Management Board
CLI	Command Line Interface
CM	Configuration Management
CRL	Certificate Revocation List
CRL DP	Certificate Revocation List Distribution Point
CVP	Content Vectoring Protocol
DES	Data Encryption Standard
DH	Diffie-Hellman
DNS	Domain Name Server
DoD	Department of Defense
ESP	Encrypted Security Payload
EAL	Evaluation Assurance Level
FIPS	Federal Information Processing Standards
FIPS PUB	FIPS Publications
FTP	File Transfer Protocol
FW	FireWall
GUI	Graphical User Interface
HFA	Hot Fix Accumulator
HMAC	Hashed Message Authentication Code
HTTP	Hypertext Transfer Protocol
ICA	Internal Certificate Authority
IDS	Intrusion Detection System
IDSSPP	Intrusion Detection System System Protection Profile
IKE	Internet Key Exchange
IP	Internet Protocol
IPS	Intrusion Prevention System

Abbreviation	Description
IPSec	Internet Protocol Security
IT	Information Technology
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
MAC	Message Authentication Code
MD5	Message Digest 5
NAT	Network Address Translation
NIC	Network Interface Card
NTP	Network Time Protocol
OCSP	Online Certificate Status Protocol
OPSEC	Open Platform for Security
OS	Operating System
OSP	Organizational Security Policy
PC	Personal Computer
PKI	Public Key Infrastructure
POP3	Post Office Protocol 3
PP	Protection Profile
PRF	Pseudo Random Function
QoS	Quality of Service
RFC	Request for Comment
RSA	Rivest, Shamir and Adleman
SA	Security Association
SFR	Security Functional Requirement
SFP	Security Function Policy
SHA-1	Secure Hash Algorithm 1
SIC	Secure Internal Communications
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
SPI	Security Parameter Index
SSH	Secure Shell
SSL	Secure Sockets Layer

Abbreviation	Description
ST	Security Target
TCP	Transmission Control Protocol
TLS	Transport Layer Security
TOE	Target of Evaluation
TSC	TSF Scope of Control
TSF	TOE Security Functions
TSP	TOE Security Policy
TSS	TOE Summary Specification
UDP	User Datagram Protocol
VLAN	Virtual LAN
VM	Virtual Machine
VPN	Virtual Private Network

2. TOE Description

2.1. Overview

Check Point VPN-1 Power/UTM provides a broad range of services, features and capabilities. This ST makes a set of claims regarding the product's security functionality, in the context of an evaluated configuration. The claimed security functionality is a subset of the product's full functionality. The evaluated configuration is a subset of the possible configurations of the product, established according to the evaluated configuration guidance.

This part of the ST describes the physical and logical scope and boundaries of the Target of Evaluation (TOE). This description effectively partitions product functionality into three classes:

- Claimed security functionality that is evaluated in the context of this ST;
- Other functionality that is in the TOE but is not evaluated in the context of this ST except for the determination that it cannot compromise any claimed security functionality;
- Excluded functionality that is not available in the TOE's evaluated configuration[10].

The TOE Description consists of the following subsections:

- **Product Types** – describes the product types of the TOE in order to give the reader a general understanding of the intended usage of the product in its evaluated configuration.
- **Physical Scope and Boundaries of the TOE** – describes hardware and software components that constitute the TOE and their relationship with the product.
- **Logical Scope and Boundaries of the TOE** – describes the IT features offered by the TOE and the product features excluded from the evaluated configuration.
- **TOE Security Functionality** – summarizes the security features of the TOE that are claimed in this ST.

[10] Note that a given product may be evaluated against more than one ST. Each ST establishes its own claimed security functionality and evaluated configuration. Functionality or product components that have been excluded from this ST may be evaluated against other security claims or evaluated in the context of different evaluated configurations.

2.2. Product Types

Check Point VPN-1 Power/UTM is a perimeter security device. The product provides controlled connectivity between two or more network environments. It mediates information flows between clients and servers located on internal and external networks governed by the firewall.

A perimeter security device is installed in its operational environment in a configuration where IP packets (datagrams) flowing between controlled networks are routed so that they pass through the perimeter security device. This allows it to inspect, allow or deny and optionally modify these information flows.

Check Point VPN-1 Power/UTM can be installed and configured to be used as the product types listed in Table 2-1 below. For each product type, column 2 specifies whether the given product type is related in this ST to claimed security functionality, corresponds to other functionality available in the TOE, or supported by the product but excluded from the TOE. Excluded product types are configurations of the product that are outside the TOE evaluated configuration. Column 3 of Table 2-1 specifies Check Point add-on products, licenses or configurations that provide the additional functionality.

Table 2-1 – Check Point VPN-1 Power/UTM Product Types

Product Type	Scope	Dependencies
Firewall	☑	
IPSec VPN gateway	☑	
Remote access / SSL[11] VPN gateway	☑	
Intrusion detection and/or prevention	☑	
Certificate management (PKI)	✓	
NAT gateway	✓	
Malicious code protection	✗	Content Inspection licenses (AV, URLF, MS)
Router	✗	Advanced Routing Suite add-on
Authorization server	✗	UserAuthority add-on
Security management product	✗	OSE, Eventia add-ons
Cooperative enforcement (NAC)	✗	Policy Server, Integrity Server add-ons
Load balancer	✗	ConnectControl add-on
QoS enforcement	✗	FloodGate add-on

Key: ☑ Claimed security functionality ✓ In TOE ✗ Excluded from TOE

[11] SSLv3.1 is equivalent to TLSv1.0. This ST uses 'SSL VPN' to denote the corresponding VPN functionality, and TLS when referring to the SSL VPN protocol used in the evaluated configuration.

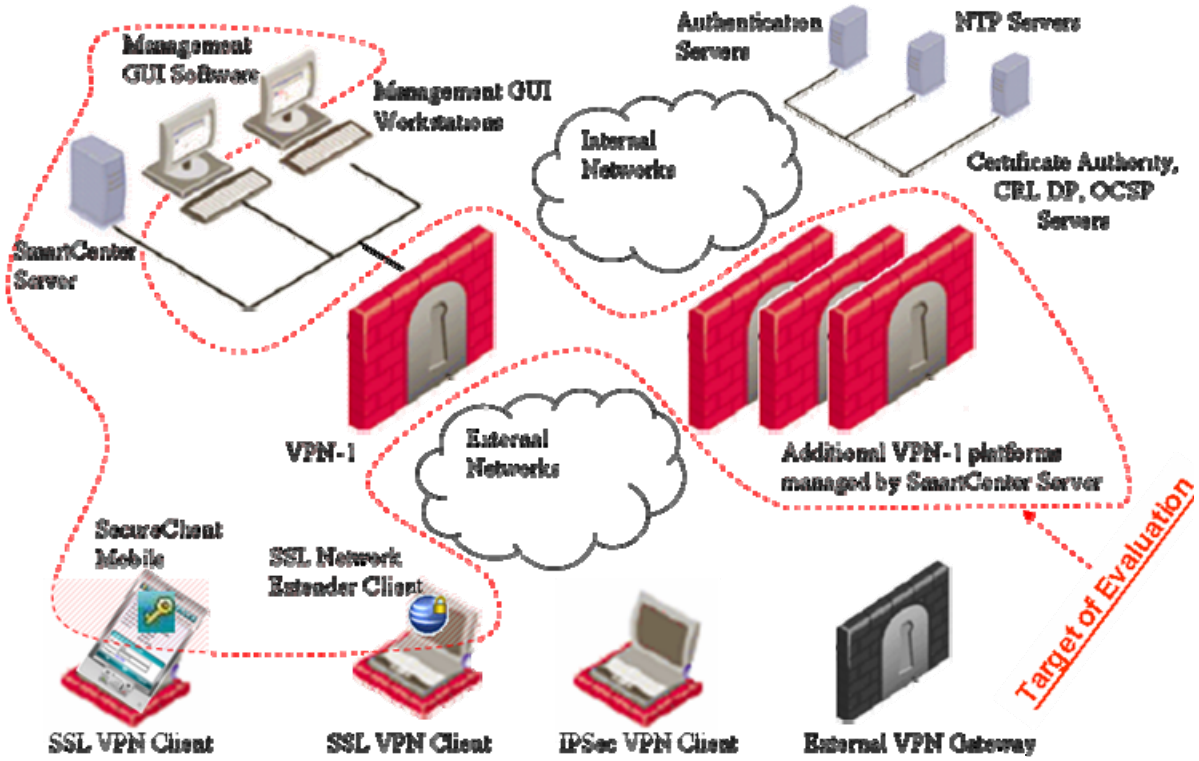
2.3. Physical Scope and Boundaries of the TOE

2.3.1. Definition

The Target of Evaluation (TOE) includes the following components:

- Check Point VPN-1 Power/UTM software; and
- Hardware platform(s) and OS on which the software is installed; and
- TOE guidance; and
- SmartCenter (Management) server software, OS and hardware; and
- Management GUI software; and
- SSL Network Extender and SecureClient Mobile (SSL VPN) client software.

Figure 2-1- Physical Scope and Boundaries of the TOE



The TOE does **not** include the following components:

- Management GUI hardware and operating system; or
- External authentication server implementing single-use authentication, if any; or
- External Certificate Authority (CA), if any; or
- External certificate validation server (HTTP or LDAP CRL DP, OCSP), if any; or
- External NTP time-synchronization server, if any; or
- IPSec VPN client, SSL VPN client hardware and operating system, if any; or
- External VPN gateways (VPN gateways not managed by the TOE).

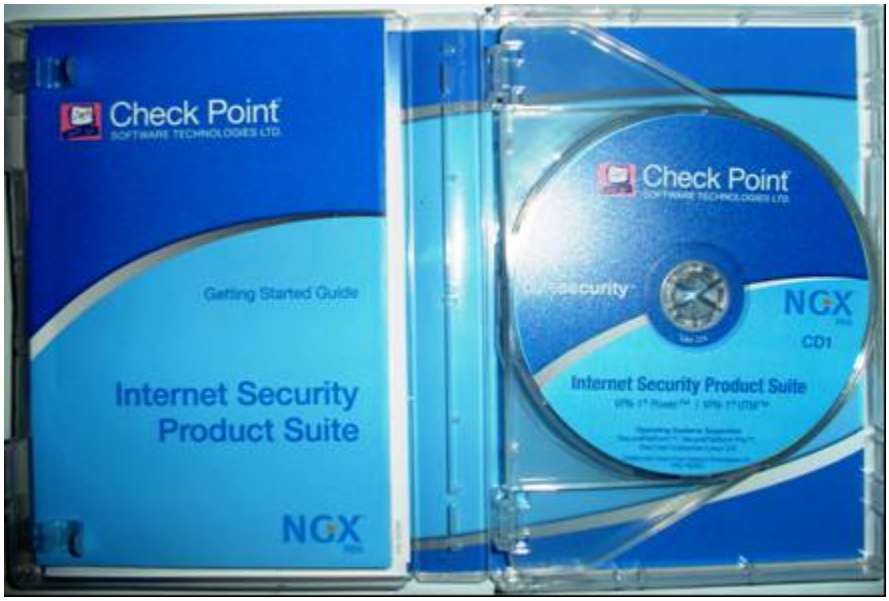
Note: Although the CD-ROM package described below includes one IPSec VPN client application (Check Point SecureClient), this application is not considered part of the TOE and is licensed separately. See section 2.3.8.3 for a partial list of supported clients.

2.3.2. TOE Software

Check Point VPN-1 Power/UTM is a software product produced by Check Point. The product is installed on a hardware platform in combination with an operating system (OS), in accordance with TOE guidance, in a FIPS 140-2 compliant mode.

The Check Point VPN-1 Power/UTM software is shipped to the consumer in a package containing CD-ROMs with the Check Point VPN-1 Power/UTM installation media and user documentation.

Figure 2-2 – Check Point VPN-1/Firewall-1 Software and Guidance Distribution



As part of its flaw remediation procedures, Check Point electronically distributes hot fix accumulators (HFAs). The HFA included in the evaluated configuration is HFA 30.

2.3.3. TOE Hardware Platforms

The consumer installs the software on commodity hardware platforms identified in Appendix A - TOE Hardware Platforms – section A.1. Alternatively, the consumer can purchase the software pre-installed on the security appliances identified in sections A.2 and A.3.

All platforms identified in Appendix A provide an AMD or Intel-based CPU as well as memory, disk, local console and network interface facilities that are tested by Check Point as providing sufficient service and reliability for the normal operation of the software. A hardware clock/timer with on-board battery backup supports the operating system in maintaining reliable timekeeping.

2.3.4. TOE Operating System

In addition to the Check Point VPN-1 Power/UTM software, an OS is installed on the hardware platform. The OS supports the TOE by providing storage for audit trail and IDS System data, an IP stack for in-TOE routing, NIC drivers and an execution environment for daemons and security servers. A large part of the product's security functionality is provided "beneath" the OS, i.e. as kernel-level code that processes incoming packets.

The software, OS and hardware platform are collectively identified in this ST as the 'Check Point VPN-1 Power/UTM appliance'.

The Check Point VPN-1 Power/UTM CD-ROM contains a Check Point proprietary OS identified as Check Point SecurePlatform[12], a stripped-down version of the Linux operating system. SecurePlatform also comes pre-installed on all Check Point security appliances.

In addition to SecurePlatform, the Check Point VPN-1 Power/UTM software can be installed on the Nokia platforms and operating systems identified in Appendix A.

2.3.5. TOE Guidance

The following Check Point guidance is considered part of the TOE:

Title	Date	Part No.
CC Evaluated Configuration Installation Guide - NGX R65	October 2008	702795
CC Evaluated Configuration Administration Guide - NGX R65	August 2008	702796
CC Evaluated Configuration User Guide - NGX R65	August 2008	702797
SecurePlatform™ /SecurePlatform Pro	February 2007	701680
SmartCenter™	January 2007	701676
Virtual Private Networks	February 2007	701675
Firewall and SmartDefense	February 2007	701682
SmartView Monitor™	February 2007	701678
VPN-1 FIPS 140-2 Non-Proprietary Security Policy, Version 1.0	October 2006	

[12] Operating system version is kept in synch with the software version. Thus both TOE software and operating system are identified by the hot fix accumulator identifier HFA 30.

2.3.6. SmartCenter Server

The Check Point VPN-1 Power/UTM media includes the SmartCenter Server management server software. The SmartCenter Server software is installed on a host together with the Check Point SecurePlatform operating system. The hardware is selected out of the list of platforms given in A.1 - Supported Hardware for Check Point SecurePlatform. The SmartCenter Server software, operating system, and hardware are considered to be part of the TOE.

A SmartCenter Server manages one or more Check Point VPN-1 Power/UTM appliances. It is used to perform management operations, to monitor the TOE's correct operation and to provide administrators with search and sort capabilities on the audit trail and IDS System data.

As described in the TOE evaluated configuration guidance, the SmartCenter Server must be installed on a protected subnet that is directly connected to a TOE Check Point VPN-1 Power/UTM appliance. The appliance protects the SmartCenter Server from any direct network access by untrusted entities.

2.3.7. Management GUI

The TOE includes three management GUI applications that are included on the Check Point VPN-1 Power/UTM media: SmartDashboard, SmartView Tracker and SmartView Monitor. These applications are installed on standard PC administrator workstations running Microsoft Windows (workstation and Windows operating system are not part of the TOE), and are used as the management interface for the TOE. The management GUI applications interact with the SmartCenter server.

The product supports the following Microsoft Windows operating systems (or later versions thereof):

- Windows 2000 Professional or Server or Advanced Server with Service Pack 3 (SP3) with Q326886 Hotfix
- Windows XP Professional SP2
- Windows Vista (Ultimate, Enterprise, Business, Home Premium, or Home Basic)
- Windows Server 2003 (Standard, Enterprise, or Datacenter Edition) SP1

The evaluated configuration includes both local and remote administration:

- *Local administration*: a management GUI is directly connected to the SmartCenter Server Local Area Network (LAN) (as in Figure 2-1 above); or
- *Remote administration*: a management GUI is installed on a protected subnet that is directly connected to a remote TOE Check Point VPN-1 Power/UTM appliance, and an IPSec VPN tunnel with Triple DES encryption is set up between the two TOE Check Point VPN-1 Power/UTM appliances protecting the management GUI and SmartCenter Server, respectively.

Figure 2-3 - Local administration of the TOE

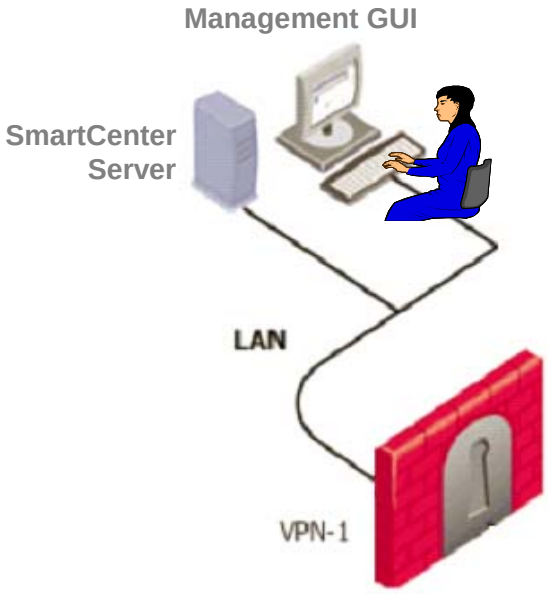
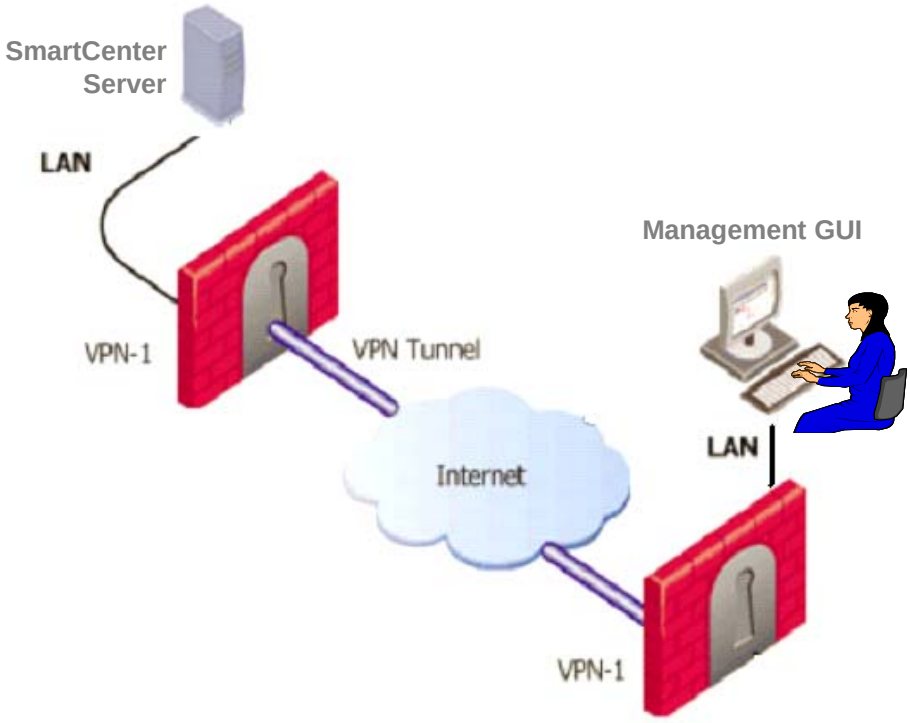


Figure 2-4 - Remote administration of the TOE



In both configurations, TOE evaluated configuration guidance requires the administrator workstation to be deployed on a protected subnet that is directly connected to a TOE Check Point VPN-1 Power/UTM appliance. The appliance protects the workstation from any network access by untrusted entities. The workstation operating system and hardware do not contribute any security functionality, and are considered to be outside the boundaries of the TOE.

2.3.8. Check Point VPN Clients

The TOE includes SSL Network Extender and SecureClient Mobile client-side software components that can be downloaded by users from a TOE appliance or manually installed in order to be able to establish SSL VPN tunnels with the TOE.

2.3.8.1. SSL Network Extender Client

The SSL Network Extender client is packaged as an ActiveX control or signed Java applet, and is installed by the user in a standard Web browser, running on standard workstation operating systems. Once installed, this lightweight client component directs remote access SSL VPN traffic between the workstation and the TOE. The client relies on operating system and cryptographic services from the underlying user workstation platform to interoperate with the TOE's SSL VPN gateway.

Figure 2-5 - SSL Network Extender running in standard Web browser

Users can download and install the SSL Network Extender client software directly from a Check Point VPN-1 Power/UTM appliance, and use it to establish the SSL VPN tunnels with the appliance. The SSL Network Extender client software packages for Microsoft Windows operating systems are part of the TOE.

The TOE also allows the user to download SSL Network Extender software packages for Linux and Mac OS X operating systems that are packaged as trusted Java applets or as a CLI. Although these variants are supported by the TOE, they are not considered to be part of the TOE, i.e. they are not being evaluated in the context of this Security Target.

The user workstation's operating system, hardware, and Web browser supporting the SSL Network Extender are considered to be outside the boundaries of the TOE.

2.3.8.2. SecureClient Mobile

SecureClient Mobile is a Check Point SSL VPN resident client that provides SSL VPN functionality on mobile platforms such as cell phones and PDAs running Windows Pocket PC and Windows Mobile operating systems. Users can download the client software package from a TOE appliance and install it on their mobile devices in order to establish SSL VPN tunnels to the TOE.

The mobile device's operating system and hardware are considered to be outside the boundaries of the TOE.

Figure 2-6 - SecureClient Mobile running on a PDA

2.3.8.3. Remote Access IPSec VPN Clients

Check Point provides a range of end point security products that provide remote access IPSec VPN capabilities compatible with the TOE, including Check Point SecureClient, Check Point Integrity SecureClient, and Check Point Endpoint Security. Some third party IPSec VPN clients have also demonstrated interoperability with the TOE.

These products can be supported in the evaluated configuration but are considered to be outside the boundaries of the TOE.

2.4. Logical Scope and Boundaries of the TOE

2.4.1. TOE Logical Interactions with its Operational Environment

The TOE supports the following logical interactions with its environment:

- **Information flow control** – users of the TOE send information through the TOE

  The TOE may perform the following interactions with its IT environment as part of its information flow control processing:

  - **Authentication queries** – the TOE queries an external authentication server in the process of authenticating a user that is requesting an information flow through the firewall
  - **Revocation queries** – the TOE queries an external directory for revocation information in the process of authenticating a user or remote IT entity using a certificate-based authentication mechanism
  - **Content verification** – the TOE passes a requested information flow that is allowed by the TOE security policy to a server in the IT environment that may perform additional content verification of the information, before the information flow is allowed to its destination
  - **Alerts** – the TOE sends alerts to external IT entities in reaction to administrator-defined events

- **VPN** – establishment of secure channels with peer IT entities:
  - **Site to Site VPN negotiation** – the TOE establishes an IPSec VPN secure channel with remote peer IT entities acting as VPN gateways
  - **Remote Access VPN negotiation** – the TOE establishes an IPSec VPN or SSL VPN secure channel with remote peer IT entities representing a human user
  - **SSL VPN client software delivery** – the TOE allows users to download SSL VPN client software (SSL Network Extender) from the TOE
- **Connectivity queries** – the TOE receives and responds to connectivity queries from external IT entities
- **Management** – authorized administrators manage the TOE and review audit trail and IDS System data via the SmartCenter Server and management GUI

  The TOE may perform the following interactions with its IT environment in the context of TOE management:

  - **IDS signature updates** – the TOE can import an IDS signatures file
- **Time synchronization** – the TOE can poll a remote NTP server to synchronize the TOE's hardware clock with other IT entities' clocks.

2.4.2. Information Flow Control

2.4.2.1. Information Flow Mediation

The TOE's primary functionality is to mediate information flows between controlled networks. In practice, information flows are processed by the TOE in the form of IPv4 packets received on any of its NICs. A TOE interface on which traffic arrives and departs may be a physical NIC, or it may be a VLAN, where incoming packets are tagged using the layer 2 IEEE 802.1Q standard (see [802.1Q]) to denote the virtual TOE interface.

The Check Point VPN-1 Power/UTM product supports IPv6; however, this support is not enabled by default, and is not enabled in the evaluated configuration.

IP packets are processed by the Check Point VPN-1 Power/UTM software[13], which associates them with application-level connections, using the IP packet header fields: source and destination IP address and port, as well as IP protocol. Fragmented packets are reassembled before they are processed.

The TOE mediates the information flows according to an administrator-defined policy. Some of the traffic may be either silently dropped or rejected (with notification to the presumed source).

Traffic may be routed through proxies (Security Servers) that process application-level traffic and originate the corresponding information flow on behalf of the communicating end points, preventing a direct connection through the TOE. The TOE provides proxies for the services: FTP, Telnet, HTTP and SMTP.

2.4.2.2. User Authentication

The TOE can be configured by an authorized administrator to require user authentication before allowing a given information flow. The product supports a number of authentication methods, including certificate-based authentication (requiring a remote access VPN connection for a given information flow), IKE shared-secret authentication, multiple-use passwords stored on the Check Point VPN-1 Power/UTM appliance, as well as authentication using an external server in the IT environment – using LDAP, RADIUS, SecurID, or TACACS protocols.

In the evaluated configuration, administrator guidance instructs the administrator to require a single-use authentication mechanism (implemented using remote access VPN, RADIUS or SecurID) for Telnet and FTP (if these services are allowed), as a condition for [APP-PP] compliance. If an external SecurID authentication server is used, it must be installed on a protected subnet that cannot be accessed by untrusted users.

[13] Check Point VPN-1 Power/UTM NGX R65 also supports a patented SecureXL interface that offloads packet processing to acceleration hardware. When an incoming IP packet matches an existing connection, for which an information flow control and/or encryption decision has already been made, that packet is processed accordingly by the hardware and is not passed on to the CPU. SecureXL is **not** supported in the evaluated configuration.

Administrators are authenticated using certificates that are issued by the Internal Certificate Authority (see below).

2.4.2.3. SmartDefense (Application Intelligence)

In addition to the IDS/IPS functionality claimed in this ST, the TOE includes an extensive set of application-level protocol compliance verification and known attack signature detection capabilities, collectively titled 'SmartDefense' or 'Application Intelligence'. These capabilities are managed using the SmartCenter Server and management GUIs, and are integrated into the product's kernel-level code.

SmartDefense code is TOE functionality that is available in the evaluated configuration but is not claimed as security functionality in this ST. The claimed IDS/IPS functionality is based on rules that are executed by the INSPECT engine (see section 2.5.2 below).

Note that ‘SmartDefense Updates’ (see section 2.4.5.2 below) are distributed as INSPECT code and are therefore considered claimed security functionality.

2.4.2.4. Information Flow Modification

Authorized information flows may be modified by the TOE, as configured by an authorized administrator. One example of this is Network Address Translation (NAT), where source and/or destination addresses and/or UDP or TCP ports are modified according to administrator-defined policies, supporting configurations where communicating end points do not interact with the actual IP address of their peers. Another example is TCP Initial Sequence Number (ISN) scrambling, which can prevent session hijacking attacks.

Information flow modification is TOE functionality that is not claimed as security functionality in this ST.

2.4.2.5. CVP and UFP

For proxied information flows, the TOE may be configured by an authorized administrator to send the information to a server in the IT environment using a Check Point proprietary Content Vectoring Protocol (CVP) or URL Filtering Protocol (UFP). This is typically used for integration with anti-virus or URL filtering products, respectively. The CVP or UFP server only receives traffic that has already been approved for forwarding by the proxy; thus it cannot cause an inappropriate information flow that would violate the TOE security policy. CVP and UFP are TOE functionality that is not claimed as security functionality in this ST.

2.4.2.6. Alerts

The authorized administrator can configure the TOE to generate alerts for selected events. Alerts can be displayed in a pop-up window on the Management GUI, or can be sent to an external IT entity as an SNMP trap or email.

2.4.3. VPN

2.4.3.1. VPN Establishment

A Check Point VPN-1 Power/UTM appliance can be configured by an authorized administrator to establish an IPSec or SSL VPN tunnel with a remote peer IT entity. The peer may be an IPSec VPN gateway such as the TOE or a third-party IPSec gateway product (site to site VPN), or it may be an IPSec or SSL VPN implementation running on a single-user client workstation (remote access VPN). The TOE identifies and authenticates the peer entity (or user) as part of the process of establishing the VPN tunnel, using the IKE protocol for IPSec VPNs, and the TLS protocol for SSL VPNs. The VPN tunnel provides protection from disclosure and undetected modification for the information flow between the peers.

2.4.3.2. VPN Communities

Management of VPN rules is performed by associating VPN peers with a VPN *community* defined by the administrator. VPN communities are defined collections of gateways, each with a defined *VPN domain*. Traffic between hosts that are in VPN domains of gateways belonging to a given community is tunneled over the VPN.

When traffic is encapsulated or decapsulated on any given tunnel, the two VPN peers that establish the tunnel uniquely identify a VPN community. The community defines the encryption methods used for all VPN tunnels established between gateways associated with the community.

A predefined Remote Access community defines encryption methods for all remote access IPSec VPN tunnels. SSL VPN encryption methods are predefined.

2.4.3.3. Use of Internal/External Certificate Authority

SmartCenter Server contains an internal certificate authority component (ICA) that is used for managing certificates used in intra-TOE communications. ICA certificates are used for securing management traffic between a SmartCenter Server and managed Check Point VPN-1 Power/UTM appliances. The ICA publishes CRLs internally to TOE components. The ICA also generates administrator certificates.

An external certificate authority in the IT environment must be used to manage VPN certificates for the TOE and its VPN peers. The TOE performs certificate revocation checks using the protocols LDAP or HTTP and also supports the OCSP protocol for performing online revocation checks.

ICA can also be used to generate certificates for external users; however, the evaluated configuration does not allow external access to the SmartCenter Server, so that certificate management for external users in the evaluated configuration must be performed in an offline manner.

2.4.3.4. IPSec DoS Protection

The TOE provides protection against denial of service (DoS) attacks that involve a large number of IKE tunnel establishment requests from unauthorized peers. When the number of concurrent requests exceeds an administrator-defined threshold, TOE IPSec VPN gateways can require the initiating peer to perform additional processing that can foil DoS attacks on the IKE protocol.

IKE DoS protection is TOE functionality that is not claimed as security functionality in this ST.

2.4.3.5. SSL Network Extender Client Download

The TOE contains a Web component that allows users to download SSL Network Extender client software components from a TOE appliance over HTTPS. Once these components are installed by the user on the user's workstation, the SSL Network Extender client directs applicable SSL VPN traffic between the workstation and the TOE.

2.4.4. Connectivity queries

The TOE responds to unauthenticated connectivity queries over ICMP, ARP, and the proprietary Check Point RDP[14] protocol. Other authenticated protocols are used for maintaining IPSec VPN tunnels.

Connectivity queries are TOE functionality that is not claimed as security functionality in this ST.

2.4.5. Management

2.4.5.1. Management Interfaces

The TOE supports both local and remote management through the SmartCenter Server. Management interfaces include the Management GUIs (SmartDashboard, SmartView Tracker and SmartView Monitor).

These interfaces allow an authorized administrator to manage the TOE rule base and general configuration, monitor its status, review audit trail and IDS System data, and manage certificates for TOE appliances as well as external users.

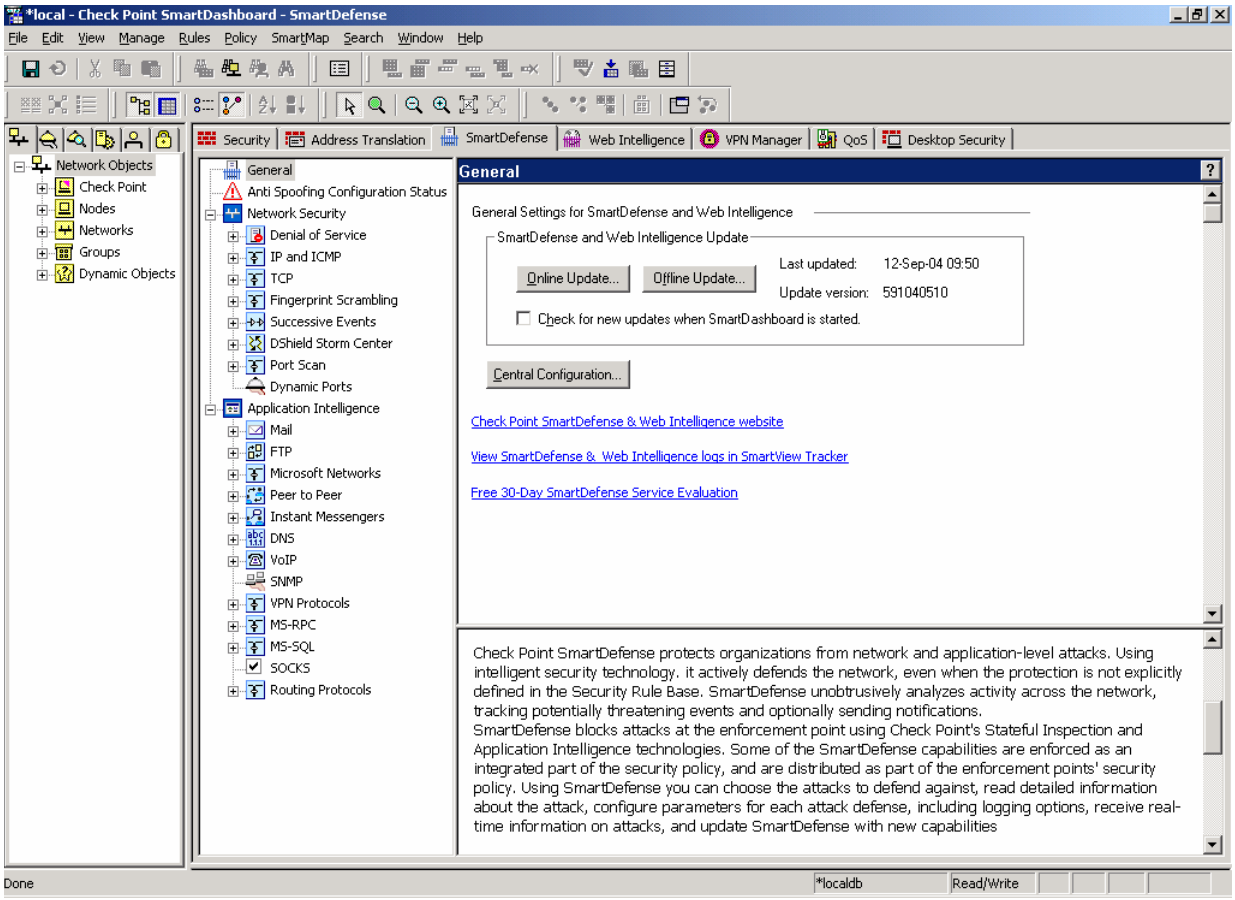
2.4.5.2. IDS Signature Updates (SmartDefense Updates)

At the request of an authorized administrator, the TOE can import attack signatures for the TOE's IDS/IPS analysis capability. This capability is named 'SmartDefense Update'. The signatures file is downloaded (outside of the TOE) over a secure channel from the Check Point Web site, and imported into the TOE as a file by the administrator.

[14] Check Point RDP is a proprietary unauthenticated UDP-based protocol (on port 259) used for VPN gateway discovery. It is not conformant with RDP as specified in RFC 908/1151.

Note that a related capability named 'SmartUpdate', which provides a software update capability, is **not** supported in the TOE evaluated configuration.

Figure 2-7 – SmartDefense Update



2.4.6. Time Synchronization

Check Point VPN-1 Power/UTM appliances contain a reliable hardware clock that provides secure timestamps for audit records and for secure channel establishment. In order to provide support for clock synchronization of multiple TOE appliances and/or external IT entities (e.g. IPSec VPN peers), the Check Point VPN-1 Power/UTM appliance includes an NTP polling agent that can be configured to interact with a remote time synchronization server in the IT environment.

If NTP time synchronization is not configured, each of the appliances in the TOE keeps its own time. The administrator can review audit records in the order in which they were received by the SmartCenter Server, with an indication of the originating component and the local time stamp. In addition, log files from each appliance are periodically forwarded to the SmartCenter Server, and can be reviewed individually.

2.4.7. Functionality Excluded from the TOE Evaluated Configuration

The Check Point VPN-1 Power/UTM product can provide a broad range of services (product types), features and capabilities. Some of these require additional products or licenses to be installed on the Check Point VPN-1 Power/UTM appliance and/or on the SmartCenter Server.

Table 2-1 above summarized services that are not part of the evaluated configuration, giving for each service the dependency on an add-on product, license, or configuration.

This section describes additional features and capabilities that are excluded from the evaluated configuration:

- **ClusterXL** – the Check Point VPN-1 Power/UTM product supports state synchronization between multiple Check Point VPN-1 Power/UTM appliances (gateway clusters) for automatic failover and load balancing between cluster members. This functionality requires the installation of the Check Point ClusterXL add-on product, and is not evaluated in the context of this ST.
- **SmartUpdate** – SmartUpdate provides a method for software updates as well as license management, allowing the system administrator to track, manage and maintain:
  - Remote upgrades of existing Check Point products
  - New installations of Check Point products on existing Check Point VPN-1 Power/UTM appliances
  - The attachment of product licenses to Check Point VPN-1 Power/UTM appliances

  SmartUpdate is implemented via a Remote Installation daemon that is disabled in the TOE evaluated configuration.
- **OPSEC client APIs** – the SmartCenter Server provides a set of APIs (and corresponding network protocols) for Check Point OPSEC partners that support integration of third-party management products. The OPSEC client APIs are not available in the TOE evaluated configuration.
- **SNMP daemon** – Check Point VPN-1 Power/UTM appliances provide optional SNMP daemons that can be used for remote management. These daemons are disabled in the TOE evaluated configuration.
- **WebUI** – the TOE operating systems provide Web-based configuration interfaces as an alternative to the Check Point VPN-1 Power/UTM appliance CLI. This interface is disabled in the TOE evaluated configuration.
- **CLIs and SSH** - Check Point VPN-1 Power/UTM appliances and operating systems include CLI interfaces that are used for initial installation and configuration of the appliance, the OS and the software. A CLI is also provided on the SmartCenter Server. The CLI can be accessed from a directly connected console or remotely using the SSH protocol.

In the evaluated configuration, these CLIs should not be used after this installation stage. All management of the TOE should be performed via the SmartCenter Server and Management GUIs. If the appliance must be reconfigured (e.g. a NIC is added to the appliance), it should be reinstalled to ensure that it remains in a secure configuration.

- **Extended Remote Access VPN Modes** - Check Point VPN-1 Power/UTM appliances support extended VPN modes that solve connectivity issues with remote access clients. The following remote access VPN modes are outside the TOE evaluated configuration:
  - **Hybrid mode** - IKE Phase I supports either certificate-based or shared secret-based authentication. Check Point VPN-1 Power/UTM supports a hybrid mode for remote access clients where the gateway authenticates using a certificate, and the client authenticates using a single-use or reusable password. Hybrid mode is outside the TOE evaluated configuration.
  - **Microsoft IPSec/L2TP clients** – the Check Point support for Microsoft IPSec/L2TP clients is outside the TOE evaluated configuration.
- **LDAP User Management** – the Check Point VPN-1 Power/UTM product supports the LDAP protocol for managing users on an external LDAP directory server. LDAP User Management requires an additional SmartDirectory license to be installed. User authentication and authorization information is retrieved from the directory over a secure channel. This configuration is not being evaluated and is outside the TOE evaluated configuration.
- **Bridge Mode** - Check Point VPN-1 Power/UTM appliances allow the administrator to configure pairs of network interfaces in bridge mode, such that layer 2 traffic picked up on one interface is transparently forwarded to the paired interface if it is allowed to flow by the Security Policy. Bridge Mode is not being evaluated and is outside the evaluated configuration.
- **DShield Storm Center** - Check Point VPN-1 Power/UTM appliances can be configured to submit rejected traffic logs to a SANS-operated center that collects malicious activity reports from a large number of contributing organizations on the Internet, and correlates these reports to produce block lists for address ranges from which such activity has been identified. The appliances can also be configured to download and apply these block lists. Evaluated configuration guidance instructs administrators not to enable this functionality, and DShield traffic is blocked by the evaluated configuration rule base.
- **Content Inspection** – in addition to providing support for external content inspection servers using the CVP and UFP interfaces, Check Point VPN-1 Power/UTM allows the administrator to enable anti-virus, URL filtering, and anti-spam components on the appliance itself, given appropriate Content Inspection licenses. Evaluated configuration guidance instructs administrators not to enable this functionality.

2.5. TOE Security Functionality

2.5.1. Summary of TOE Security Functionality

Check Point VPN-1 Power/UTM mediates information flows between clients and servers located on internal and external networks governed by the firewall. Proxy servers on the firewall, for the services FTP and Telnet, require authentication by client users before requests for such services can be authorized.

User authentication may be achieved by a remote access client authenticating using IKE or TLS, against public key or shared-secret credentials held by the user. Alternatively, proxy servers are configured by the authorized administrator to require the user to enter a single-use password and forward it to a RADIUS or SecurID server for validation. Thus, only valid requests are relayed by the proxy server to the actual server on either an internal or external network.

Proxies are also provided for the services SMTP and HTTP that can optionally, as determined by the authorized administrator, require the client user to authenticate.

The product additionally imposes traffic-filtering controls on mediated information flows between clients and servers according to the site's security policy rules. By default, these security policy rules deny all inbound and outbound information flows through the TOE. Only an authorized administrator has the authority to change the security policy rules.

Once an authorized administrator describes the network topology in terms of networks and IP addresses, anti-spoofing controls prevent information flows that contain invalid source addresses, i.e. source addresses that should not be received by the TOE interface on which the information flow has arrived.

An IDS/IPS capability is integrated with the product's traffic-filtering functionality, matching traffic with predefined attack signatures, and providing recording, analysis, and reaction capabilities.

IPSec VPN and SSL VPN capabilities are provided to encrypt network traffic to and from selected peers, in order to protect traffic from disclosure or modification over untrusted networks. External IT entities establishing VPN tunnels with the TOE can be VPN gateways such as the TOE (site to site VPN), or may be single-user client workstations (remote access VPN). The VPN identifies and authenticates the peer entity as part of the process of establishing the VPN tunnel, via the IKE or TLS protocols, respectively.

Administrators authenticate to the TOE using a certificate-based authentication mechanism before they can use the Management GUIs to access the SmartCenter Server. Authorized administrators can perform both local and remote management of the TOE. An IPSec VPN tunnel using FIPS 140-2 compliant Triple DES encryption is used to protect remote management sessions.

Administrator sessions are protected via a trusted path between the Management GUI and the SmartCenter Server. Internal TOE communications between the SmartCenter Server and Check Point VPN-1 Power/UTM appliances is also protected from disclosure and undetected modification.

Audit trail data is stamped with a dependable date and time when recorded. Auditable events include modifications to the group of users associated with the authorized administrator role, all use of the identification and authentication mechanisms (including any attempted reuse of authentication data), all information flow control decisions made by the TOE according to the security policy rules, and the use of all security functions. If the audit trail becomes filled, then the only auditable events that may be performed are those performed by the authorized administrator. The TOE includes tools to perform searching and sorting on the collected audit trail data according to attributes of the data recorded and ranges of some of those attributes.

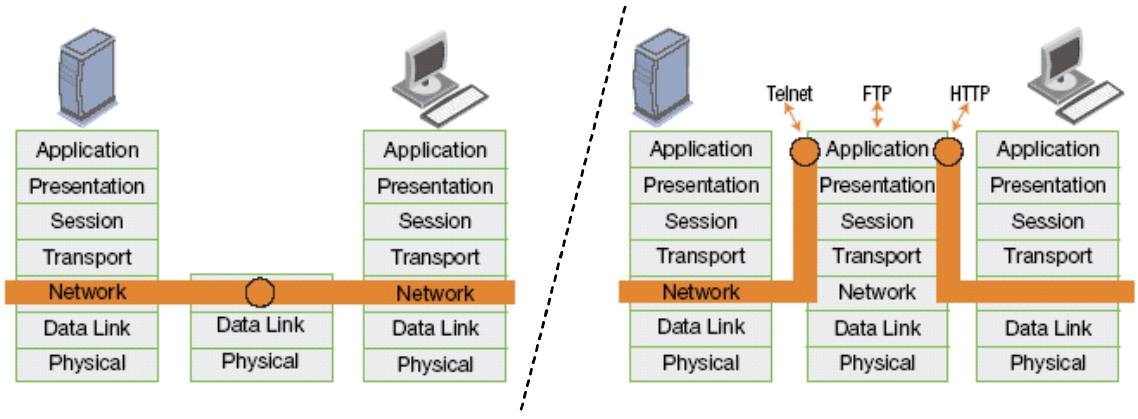
The Check Point VPN-1 Power/UTM appliance protects itself and the SmartCenter Server and Management GUIs against network-level attacks by unauthorized users, with a medium robustness. Domain separation is provided between TOE interfaces. Self tests are run during initial start-up and periodically during normal operation to ensure correct operation. A hardware clock provides reliable timestamps. Management communication between Check Point VPN-1 Power/UTM appliances and the SmartCenter Server is protected against disclosure and modification.

2.5.2. Firewall Functionality and Stateful Inspection

The purpose of a firewall is to provide controlled and audited access to services, both from inside and outside an organization's network, by allowing or denying the flow of data through the firewall. Although there are a number of firewall architectures and technologies, firewalls basically fall into two major categories: traffic-filter and application-level firewalls.

Traffic filters are capable of screening network traffic at the network and transport protocol levels. Application-level firewalls perform a similar task, but at the application level, using proxies that process application-level traffic and originate the corresponding information flow on behalf of the communicating end points, preventing a direct connection through the firewall. While Application-level firewalls arguably provide a higher level of security functionality, they pay a penalty in performance and flexibility.

Figure 2-8- Traffic filtering (left) vs. Application-level Proxies



Check Point VPN-1 Power/UTM provides both traffic-filtering capabilities and application-level proxies. In addition, the product provides a capability for Stateful

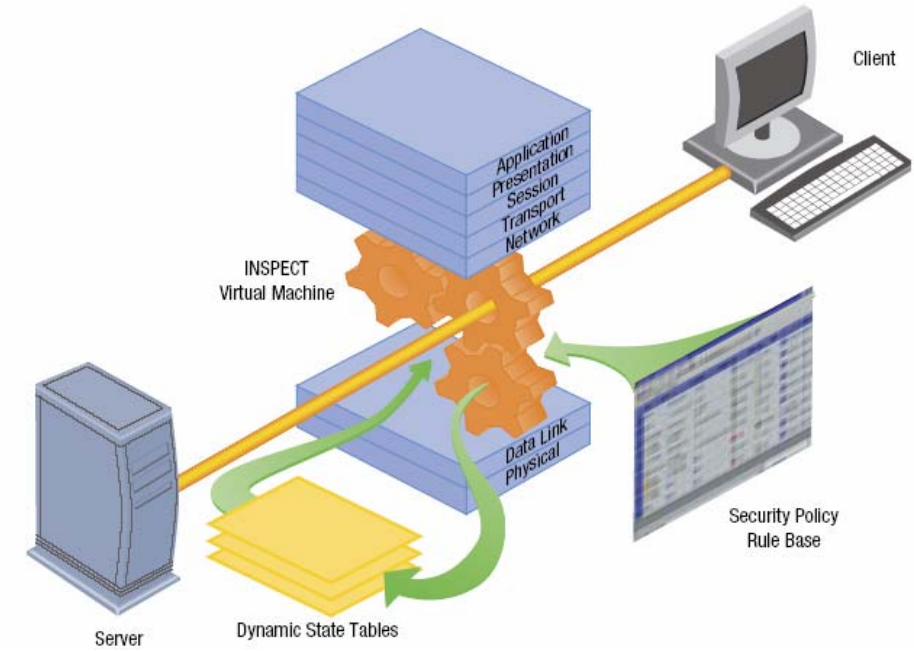
Inspection. With Stateful Inspection, packets are intercepted at the network layer (as in a traffic filter), but the firewall can inspect any information in the packet, at all layers of the network stack. Stateful Inspection then incorporates communication-and application-derived state and context information which is stored and updated dynamically. This provides cumulative data against which subsequent communication attempts can be evaluated.

For example, a rule configured by an authorized administrator to allow DNS UDP traffic to flow to a naming server implies that the reply packet should be let through. When the DNS request is allowed through the firewall, the firewall expects to see the reply packet within a given timeout period, and sets up a connection state accordingly. When the reply packet flows back through the firewall, the firewall allows it to go through and deletes the connection state.

Check Point's Stateful Inspection architecture utilizes a patented INSPECT Engine which enforces the security policy on the firewall. The INSPECT Engine looks at all communication layers and extracts only the relevant data, enabling highly efficient operation, support for a large number of protocols and applications, and easy extensibility to new applications and services.

The INSPECT engine is implemented in the Check Point VPN-1 Power/UTM appliance as a kernel-level virtual machine. Security policy is compiled on the SmartCenter Server into virtual machine inspection code that is downloaded to the appliance. The inspection code operates on incoming packets before they even reach the operating system IP stack.

Figure 2-9 - Stateful Inspection



2.5.3. Security Rule Base

The TOE's firewall and VPN capabilities are controlled by defining an ordered set of rules in the Security Rule Base. The Rule Base specifies what communication will be allowed to pass and what will be blocked. It specifies the source and destination of the communication, what services can be used, at what times, whether to log the connection and the logging level.

Figure 2-10- Example Rule

SOURCE	DESTINATION	VPN	SERVICE	ACTION	TRACK	INSTALL ON	TIME
Alaska.LAN	Any	Any Traffic	http	accept	Log	Policy Targets	Any

2.5.4. Traffic filtering and Intrusion Detection/Prevention

The TOE's traffic filtering and IDS/IPS capabilities are based on the INSPECT engine. Traffic filtering matches traffic headers with administrator-defined rules, which allow, drop, or reject (notifying the traffic source) incoming packets.

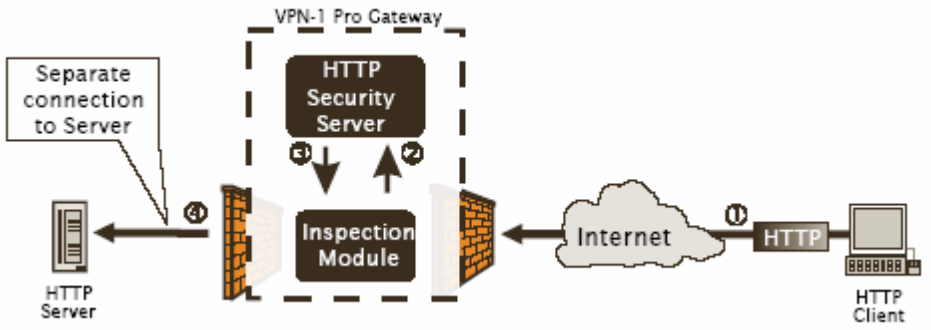
IDS/IPS functionality involves matching packets that have been allowed by the TOE's firewall and VPN policies against predefined attack signatures that may match any packet content, and may take into account state information. When a packet matches a signature, the TOE may record the packet, drop or reject it.

IDS signatures may be defined manually by the administrator, or downloaded from a Check Point subscription service (see section 2.4.5.2 above). Signature updates are installed as INSPECT code fragments, and are packaged with corresponding GUI updates to integrate seamlessly with previously installed defenses.

2.5.5. Security Servers

Proxies are implemented as security server processes. The TOE provides security servers for the protocols FTP, telnet, HTTP and SMTP. When an incoming packet matches a rule for one of these protocols, the virtual machine transfers the packet to be processed by an appropriate security server. Security servers verify conformance with the appropriate protocol. Multiple security servers may be spawned for a given protocol.

Figure 2-11- Security Servers

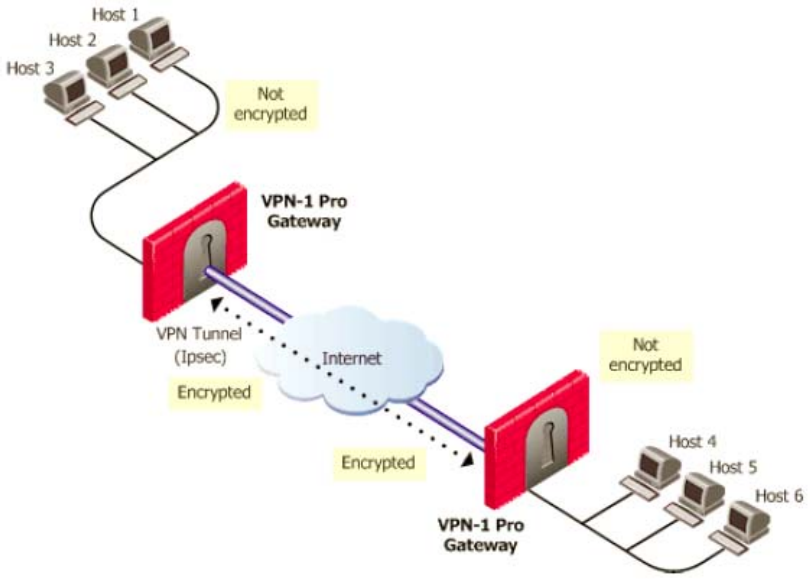


2.5.6. Virtual Private Networking (VPN)

A VPN provides the ability to use a public or untrusted network, such as the Internet, as if it were a secure, private network. A VPN is created through the use of devices that can establish secure communication channels over a common communications infrastructure, protecting data in-transit between two communicating entities. The secure communications channels are established using security mechanisms defined by the IPSec and IKE, or TLS Internet standards.

The VPN is established by a device at each enclave boundary. Each device authenticates itself to its peer, agrees upon cryptographic keys and algorithms, securely generates and distributes session keys as necessary, and encrypts network traffic in accordance with the defined security policy.

Figure 2-12- Virtual Private Network



A VPN community is defined as a collection of VPN gateways. Topology definitions created by the authorized administrator associate each VPN gateway (a TOE appliance) with a VPN domain, i.e. a defined set of IP addresses for which the gateway decapsulates VPN traffic. VPN community definitions control what traffic is tunneled, and what VPN methods and algorithms are used to protect the tunneled traffic.

When traffic flows out through a gateway from its VPN domain, the gateway determines from the defined topology whether the presumed destination address lies in the VPN domain of a VPN peer; if it does, the gateway uses the security attributes defined for the VPN community that includes both gateways (a pair of gateways cannot be defined in more than one VPN community) in order to determine whether to tunnel the traffic to the VPN peer, and to select appropriate VPN mechanisms and algorithms.

Conversely, tunneled traffic received by the gateway from a VPN peer is decrypted and verified using the corresponding VPN community security attributes, before being forwarded to its presumed destination address.

VPN community topology may be either Meshed (see Figure 2-13), where any traffic between VPN domains of the community's gateways is tunneled, Star (see Figure 2-14), where traffic between satellite gateways and central gateways is tunneled, or Remote Access, where the TOE establishes VPN tunnels with remote access clients acting on behalf of a remote access user.

VPN community topologies may be combined (e.g. a star where each satellite is a meshed community). This allows the administrator to control complex VPN architectures without having to resort to manually defining each VPN tunnel created between any two gateways.

Figure 2-13- Example of a Meshed VPN Community

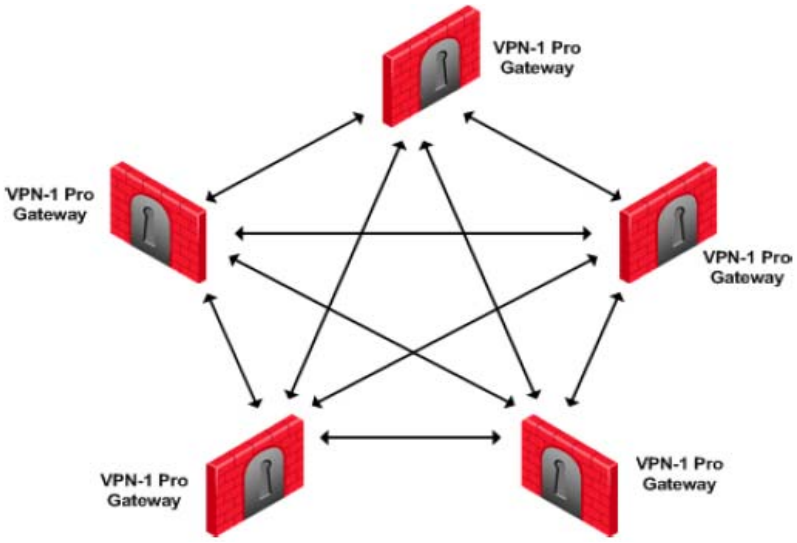
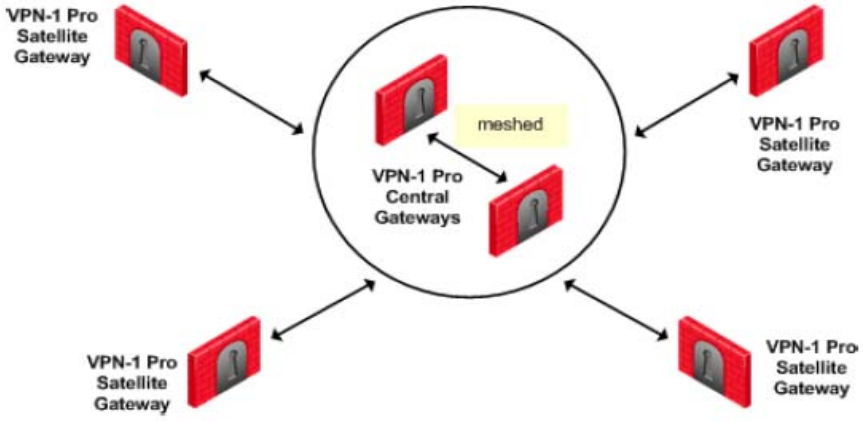


Figure 2-14- Example of a Star VPN Community



VPN community settings are orthogonal to the Rule Base; the Rule Base determines what traffic is allowed to pass through the gateway. VPN communities control how allowed traffic is allowed to flow between gateways.

In the example given in Figure 2-15 below, the gateways protecting management hosts have been defined in a VPN community named 'CPMI_Community'; the example rule

will only match CPMI traffic from GUI clients to the management server that has been tunneled using the 'CPMI_Community' VPN community. Other CPMI traffic (e.g. unencrypted traffic) will not be allowed by this rule.

Figure 2-15- VPN community used as a Rule Base security attribute

2.5.7. Secure Internal Communications (SIC)

All internal communications between the Management GUI and the SmartCenter Server, between the SmartCenter Server and Check Point VPN-1 Power/UTM appliances as well as communications with remote trusted IT entities that interact with the TOE using OPSEC APIs (i.e. CVP or UFP servers) are protected using a Secure Internal Communications mechanism that is based on the TLS protocol. Certificates for SIC are generated and managed by the Internal Certificate Authority (ICA).

2.6. Check Point Services

2.6.1. Check Point User Center

Users of the TOE register with the Check Point User Center, a resource on the Check Point Web site that allows the users to manage their Check Point product licenses, to receive Check Point news and notifications, to interact with Check Point support, and to receive additional Check Point services.

User Center registration is open to all users. Some User Center services are provided only to users that have purchased suitable recurring licenses. The following subsections describe those services that are related to the security claims made in this ST.

2.6.2. SecureKnowledge Solutions

SecureKnowledge is a self-service database designed to answer user questions on technical installation, configuration, and troubleshooting for Check Point products. SecureKnowledge Solutions (SKs) may also contain additional documents, scripts or utilities that users may download to assist in performing tasks outlined in the SK.

The SecureKnowledge database provides two levels of access: General Access, and Advanced Access. The former level is available to all User Center accounts; the latter level is available only to users who purchase an Enterprise Support program, in addition to their Enterprise Software Subscription (see below).

SecureKnowledge Solution sk35763 provides resources related to this evaluation. It is available for General Access.

2.6.3. Check Point Release Notification

Users with a User Center account may register to receive Check Point Release Notifications, which are HTML e-mails that provide up-to-date information about hot-fixes, new releases, updated SecureKnowledge Solutions, and other important information. Check Point Release Notifications are available to any customer regardless of current support status.

If Check Point discovers a security flaw that might require corrective action on behalf of the customer, it will publish guidance on implementing the recommended solution and/or corrective hot-fixes via the Release Notifications mechanisms.

2.6.4. Enterprise Software Subscription

TOE users must purchase an Enterprise Software Subscription license to be eligible to download new releases of Check Point VPN-1 Power/UTM software, including hot fixes, service packs and major upgrades.

2.6.5. SecureTrak Service

The SecureTrak service allows users with a User Center account to create and track Service Requests (SRs). All TOE users can use this service to report suspected security

flaws. All security flaw reports are investigated; however, only customers that purchase a an Enterprise Support program are guaranteed a direct response, in accordance with their Service Level Agreement (SLA).

2.6.6. SmartDefense Services

TOE users may purchase a recurring subscription to Check Point SmartDefense Services. SmartDefense Services are backed by the Check Point SmartDefense Research Center, a global team of security researchers located in three main security centers – San Francisco, Tel Aviv and Minsk – providing 24-hour research and coverage.

The SmartDefense Research Center conducts original research on network, protocol and application vulnerabilities. It also actively monitors various communities to identify vulnerabilities and potential exploits that might affect IT products used by Check Point customers, before they are introduced into the "wild" (i.e., to the general Internet community). SmartDefense Services provide Check Point customers with up-to-date defenses against new attacks.

SmartDefense Updates are made available on the Check Point Web site for licensed customers. SmartDefense Updates contain packaged INSPECT code that updates the IDS/IPS functionality of the Check Point VPN-1 Power/UTM software and corresponding Management GUI controls, allowing the authorized administrator to enable specific defenses against known attack signatures that have been identified by the SmartDefense Research Center.

In addition, licensed SmartDefense Services customers receive Security Best Practices and SmartDefense Advisories that contain the latest security recommendations from Check Point, including detailed descriptions and step-by-step instructions on how to activate and configure relevant defenses provided by Check Point products and SmartDefense Updates.

3. TOE Security Environment

3.1. Assumptions

The following conditions are assumed to exist in the operational environment (identical to the set of assumptions made in both [APP-PP] and [TFF-PP], provided here for the benefit of the reader of the ST):

A.PHYSEC The TOE is physically secure.

A.MODEXP The threat of malicious attacks aimed at discovering exploitable vulnerabilities is considered moderate.

A.GENPUR There are no general-purpose computing capabilities (e.g., the ability to execute arbitrary code or applications) and storage repository capabilities on the TOE.

A.PUBLIC The TOE does not host public data.

A.NOEVIL Authorized administrators are non-hostile and follow all administrator guidance; however, they are capable of error.

A.SINGEN Information can not flow among the internal and external networks unless it passes through the TOE.

A.DIRECT Human users within the physically secure boundary protecting the TOE may attempt to access the TOE from some direct connection (e.g., a console port) if the connection is part of the TOE.

A.NOREMO Human users who are not authorized administrators can not access the TOE remotely from the internal or external networks[15].

A.REMACC Authorized administrators may access the TOE remotely from the internal and external networks.

3.2. Threats to Security

This section describes the threats that are addressed either by the TOE or the environment. These include threats that are defined in the firewall PPs, as well as threats that are countered by the TOE's IDS and VPN functionality.

3.2.1. Firewall-related Threats

The following threats are identified in both [APP-PP] and [TFF-PP] (provided here for the benefit of the reader of the ST). The threat agents are either unauthorized persons or external IT entities not authorized to use the TOE itself.

[15] This assumption means that the TOE does not provide remote services to human users, other than use of identification and authentication functions. The objective for the non-IT environment O.NOREMO upholds this assumption. Note however that both PPs allow the TOE to provide a limited number of security functions to remote (identified and authenticated) authorized external IT entities. These are listed in section 2.4.1 above.

T.NOAUTH	An unauthorized person may attempt to bypass the security of the TOE so as to access and use security functions and/or non-security functions provided by the TOE.
T.REPEAT	An unauthorized person may repeatedly try to guess authentication data in order to use this information to launch attacks on the TOE.
T.REPLAY	An unauthorized person may use valid identification and authentication data obtained to access functions provided by the TOE.
T.ASPOOF	An unauthorized person on an external network may attempt to by-pass the information flow control policy by disguising authentication data (e.g., spoofing the source address) and masquerading as a legitimate user or entity on an internal network.
T.MEDIAT	An unauthorized person may send impermissible information through the TOE which results in the exploitation of resources on the internal network.
T.OLDINF	Because of a flaw in the TOE functioning, an unauthorized person may gather residual information from a previous information flow or internal TOE data by monitoring the padding of the information flows from the TOE.
T.PROCOM	An unauthorized person or unauthorized external IT entity may be able to view, modify, and/or delete security related information that is sent between a remotely located authorized administrator and the TOE.
T.AUDACC	Persons may not be accountable for the actions that they conduct because the audit records are not reviewed, thus allowing an attacker to escape detection.
T.SELPRO	An unauthorized person may read, modify, or destroy security critical TOE configuration data.
T.AUDFUL	An unauthorized person may cause audit records to be lost or prevent future records from being recorded by taking actions to exhaust audit storage capacity, thus masking an attackers actions.
T.MODEXP	A skilled attacker with moderate attack potential may attempt to bypass the TSF to gain access to the TOE or the assets it protects.
T.TUSAGE	The TOE may be inadvertently configured, used, and administered in an insecure manner by either authorized or unauthorized persons.

3.2.2. IDS-related Threats

[IDSSPP] objectives are generally remapped in this ST to threats defined in the firewall PPs, and are mostly not redefined here (see rationale Table 8-1 for mapping).

The following threats are included from the [IDSSPP] because they complement T.MEDIAT to reflect aspects of the security problem that demonstrate the synergy between the TOE's firewall and IDS/IPS functionality. Note that the IT System that the TOE monitors is the network, and indirectly the resources on the network.

T.MISUSE Unauthorized accesses and activity indicative of misuse may occur on an IT System the TOE monitors.

T.INADVE Inadvertent activity and access may occur on an IT System the TOE monitors.

T.MISACT Malicious activity, such as introductions of Trojan horses and viruses, may occur on an IT System the TOE monitors.

3.2.3. VPN-related Threats

The following threats are countered by the TOE's VPN functionality.

T.NACCESS An unauthorized person or external IT entity may be able to view data that is transmitted between the TOE and a remote authorized external IT entity.

T.NMODIFY An unauthorized person or external IT entity may modify data that is transmitted between the TOE and a remote authorized external IT entity.

3.3. Organizational Security Policies

Both [APP-PP] and [TFF-PP] define the following OSP:

Federal agencies are required to protect sensitive but unclassified information with cryptography. Products and systems compliant with this Protection Profile are expected to utilize cryptographic modules for remote administration compliant with FIPS PUB 140-1 (level 1).

P.CRYPTO Triple DES encryption (as specified in FIPS 46-3 [3]) must be used to protect remote administration functions, and the associated cryptographic module must comply, at a minimum, with FIPS 140-1 (level 1).

4. Security Objectives

4.1. Information Technology (IT) Security Objectives

The IT security objectives defined in this ST include both the objectives defined in the claimed PPs, as well as objectives that require the TOE to provide VPN functionality.

4.1.1. Firewall PP Objectives

The following IT security objectives for the TOE are identical to the set of security objectives defined in [APP-PP] and in [TFF-PP], except for the exceptions listed below:

- The term 'and data' has been added to the definition of O.IDAUTH to ensure that the objective as stated is inclusive of the corresponding [IDSSPP] objective.
- Objective O.MEDIATE defined in [APP-PP] expands a corresponding objective from [TFF-PP]. The [APP-PP] definition is used in this ST.
- For O.EAL, a higher assurance objective has been selected for this ST than is required by either [APP-PP] or [TFF-PP].

O.IDAUTH The TOE must uniquely identify and authenticate the claimed identity of all users, before granting a user access to TOE functions and data or, for certain specified services, to a connected network.

Application Note: *Note that in view of the guidance given by [PD-0115], a corresponding objective for the IT environment OE.IDAUTH has been added to support the optional use by the TSF of authentication components such as RADIUS in the IT environment.*

O.SINUSE The TOE must prevent the reuse of authentication data for users attempting to authenticate to the TOE from a connected network.

O.MEDIAT The TOE must mediate the flow of all information between clients and servers located on internal and external networks governed by the TOE, disallowing passage of non-conformant protocols and ensuring that residual information from a previous information flow is not transmitted in any way.

O.SECSTA Upon initial start-up of the TOE or recovery from an interruption in TOE service, the TOE must not compromise its resources or those of any connected network.

O.ENCRYP The TOE must protect the confidentiality of its dialogue with an authorized administrator through encryption, if the TOE allows administration to occur remotely from a connected network.

O.SELPRO The TOE must protect itself against attempts by unauthorized users to bypass, deactivate, or tamper with TOE security functions.

O.AUDREC The TOE must provide a means to record a readable audit trail of security-related events, with accurate dates and times, and a means to search and sort the audit trail based on relevant attributes.

O.ACCOUN	The TOE must provide user accountability for information flows through the TOE and for authorized administrator use of security functions related to audit.
O.SECFUN	The TOE must provide functionality that enables an authorized administrator to use the TOE security functions, and must ensure that only authorized administrators are able to access such functionality.
O.LIMEXT	The TOE must provide the means for an authorized administrator to control and limit access to TOE security functions by an authorized external IT entity.
O.EAL	The TOE must be methodically tested and shown to be resistant to attackers possessing moderate attack potential.

4.1.2. IDS PP Objectives

The following IT security objectives for the TOE are identical to the set of security objectives defined in [IDSSPP], except for the exceptions listed below that have been omitted in this ST because they are not needed to establish the [IDSSPP] IT security requirements (see omission rationale in section 8.1.1.2):

- O.PROTCT – similar to objective O.SELPRO defined above.
- O.IDSCAN – irrelevant as the TOE does not perform scanning; only sensing.
- O.EADMIN and O.ACCESS- included in objective O.SECFUN defined above.
- O.IDAUTH – subsumed by objective O.IDAUTH defined above.
- O.AUDITS – generalized by objective O.AUDREC defined above.
- O.EXPORT - omitted as per the guidance given by [PD-0097].

O.IDSENS	The Sensor must collect and store information about all events that are indicative of inappropriate activity that may have resulted from misuse, access, or malicious activity of IT System assets and the IDS.
O.IDANLZ	The Analyzer must accept data from IDS Sensors or IDS Scanners and then apply analytical processes and information to derive conclusions about intrusions (past, present, or future).
O.RESPON	The TOE must respond appropriately to analytical conclusions.
O.OFLOWS	The TOE must appropriately handle potential audit and IDS System data storage overflows.
O.INTEGR	The TOE must ensure the integrity of all audit and IDS System data.

4.1.3. VPN Objectives

The following IT security objective models the TOE's VPN functionality:

O.VPN	The TOE must be able to protect the integrity and confidentiality of data transmitted to a peer authorized external IT entity via encryption and pro-

vide authentication for such data. Upon receipt of data from a peer authorized external IT entity, the TOE must be able to decrypt the data and verify that the received data accurately represents the data that was originally transmitted.

4.2. Security Objectives for the Environment

The assumptions made in [APP-PP] and [TFF-PP] about the TOE's operational environment must be upheld by corresponding non-IT security objectives for the environment.

In addition, the TOE's ability to set up security associations with peer authorized external IT entities depends on the peer's enforcement of a compatible security policy and its compatibility with the TOE's secure channel implementation.

Per the guidance given in [PD-0115], this ST defines an IT security objective for the IT environment, OE.IDAUTH, in order to support the use of authentication components such as RADIUS in the IT environment.

4.2.1. Firewall PP Non-IT Security Objectives for the Environment

The following non-IT security objectives are identical[16] to the corresponding objectives defined in [APP-PP] and [TFF-PP], which 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 are intended to be satisfied largely through application of procedural or administrative measures.

NOE.PHYSEC	The TOE is physically secure.
NOE.MODEXP	The threat of malicious attacks aimed at discovering exploitable vulnerabilities is considered moderate.
NOE.GENPUR	There are no general-purpose computing capabilities (e.g., the ability to execute arbitrary code or applications) and storage repository capabilities on the TOE.
NOE.PUBLIC	The TOE does not host public data.
NOE.NOEVIL	Authorized administrators are non-hostile and follow all administrator guidance; however, they are capable of error.
NOE.SINGEN	Information cannot flow among the internal and external networks unless it passes through the TOE.
NOE.DIRECT	Human users within the physically secure boundary protecting the TOE may attempt to access the TOE from some direct connection (e.g., a console port) if the connection is part of the TOE.

[16] The non-IT security objectives in this ST are identical to the corresponding objectives defined in the PPs, with the exception of the different labeling convention used in this ST to denote non-IT security objectives, e.g. NOE.GENPUR rather than O.GENPUR.

NOE.NOREMO Human users who are not authorized administrators cannot access the TOE remotely from the internal or external networks.

NOE.REMACC Authorized administrators may access the TOE remotely from the internal and external networks.

NOE.GUIDAN The TOE must be delivered, installed, administered, and operated in a manner that maintains security.

NOE.ADMTRA Authorized administrators are trained as to establishment and maintenance of security policies and practices.

4.2.2. IDS PP Non-IT Objectives for the Environment

Except for NOE.CREDEN defined below, the IDS PP security objectives for the environment parallel the Firewall PP objectives, as follows:

IDS-PP Objective for the Environment	Corresponding Objective in this ST
O.INSTAL	NOE.GUIDAN
O.PHYCAL	NOE.PHYSEC
O.CREDEN	NOE.CREDEN
O.PERSON	NOE.NOEVIL, NOE.ADMTRA
O.INTROP	As this IDS is analyzing network traffic, this is equivalent to objective NOE.SINGEN.

NOE.CREDEN defined in [IDSSPP] should be applicable to the Firewall PPs as well, and does not serve to violate the original intent of the Firewall PP assumptions[17].

NOE.CREDEN Those responsible for the TOE must ensure that all access credentials are protected by the users in a manner which is consistent with IT security.

4.2.3. Firewall PP Security Objectives for the IT Environment

OE.IDAUTH The IT environment must be able to support the unique authentication of the claimed identity of users, before a user is granted access, for certain specified services, to a connected network.

[17] Guidance on the effect of the addition of environmental assumptions on PP compliance is given in [PD-0055].

4.2.4. VPN Security Objectives for the IT Environment

OE.VPN	Peer external IT entities must be able to protect the integrity and confidentiality of data transmitted to the TOE via encryption and provide authentication for such data. Upon receipt of data from the TOE, the peer external IT entity must be able to decrypt the data and verify that the received data accurately represents the data that was originally transmitted.

5. IT Security Requirements

5.1. TOE Security Functional Requirements

The functional security requirements (SFRs) for this ST consist of the following components from CC Part 2 with the addition of extended components (EXP), summarized in the following table.

The requirements were drawn from both [APP-PP] and [TFF-PP]; requirements have also been added to address the VPN objectives. The source for each requirement is denoted in column 3 of Table 5-1 as follows:

APP Requirement drawn from [APP-PP].

TFF Requirement drawn from [TFF-PP].

IDS Requirement drawn from [IDSSPP].

Both Requirement is identical in both [APP-PP] and [TFF-PP].

All Requirement is equivalent in [APP-PP], [TFF-PP] and [IDSSPP].

DEP Requirement is defined in CC Part 2 as a dependency of a stated PP requirement, and is therefore included in this ST.

VPN Requirement added to address VPN objectives

Other Requirement added to support other, existing objectives

The CC defined operations of assignment, selection, and refinement were applied in relation to the requirements specified in the Firewall PPs as described in column 4 of Table 5-1 below, and in relation to the IDS System PP as described in column 5. In addition, columns 4 and 5 identify PP components for which a hierarchical component was selected in this ST. For components that were not drawn from any of the claimed PPs, assignment, selection and refinement operations are described in relation to the corresponding [CC] Part 2 requirement. Explicitly stated extended requirements (EXP) are identified as 'Explicit' in the appropriate CC Operations Applied column. The application of the CC iteration operation is identified in column 1 of the table.

Both firewall PPs require that the TOE satisfy a minimum strength of function ‘SOF-medium’. The only applicable security functional requirement is FIA_UAU.5.

* Application Note: *Both protection profiles [APP-PP] and [TFF-PP] specify an SFP identified as UNAUTHENTICATED SFP. However, this SFP is an application proxy SFP in [APP-PP], and a traffic filter SFP in [TFF-PP]. To avoid confusion, the corresponding [TFF-PP] information flow SFRs have been renamed to FDP_IFC.1(3) and FDP_IFF.1(3), and the corresponding SFP renamed as TRAFFIC FILTER SFP. Where an SFR refers to UNAUTHENTICATED SFP in both PPs that SFR was **refined** to refer to both the UNAUTHENTICATED SFP and to the TRAFFIC FILTER SFP.*

Table 5-1 –Security functional requirement components

Functional Component		Source PP(s)	CC Operations Applied	
			Firewall PP	IDS PP
FAU_GEN.1	Audit data generation	All	Refinement	Refinement
FAU_GEN.2	User identity association	Other	None	
FAU_SAA.3	Simple attack heuristics	Other	Assignment	
FAU_SAR.1	Audit review	All	Refinement, assignment	Refinement, assignment
FAU_SAR.2	Restricted audit review	IDS		None
FAU_SAR.3	Selectable audit review	All	Assignment	Refinement, assignment
FAU_SEL.1	Selective audit	IDS		Assignment
FAU_STG.2	Guarantees of audit data availability	All	Hierarchical[18], refinement	Refinement, assignment, selection
FAU_STG.3	Action in case of possible audit data loss	Other	Refinement, assignment	
FAU_STG.4	Prevention of audit data loss	All	Refinement	Refinement, selection
FCS_CKM.2(1)	Cryptographic key distribution	VPN	Refinement, assignment	
FCS_CKM.2(2)		Other	Refinement, assignment	
FCS_COP.1(1)	Cryptographic operation	Both	None	
FCS_COP.1(2)		Other	Assignment	
FCS_COP.1(3)		VPN	Assignment	
FCS_COP.1(4)		VPN	Assignment	
FCS_COP.1(5)		Other	Assignment	
FCS_COP.1(6)		Other	Assignment	
FCS_COP.1(7)		VPN	Assignment	
FDP_IFC.1(1)	Subset information flow control	APP	Refinement	
FDP_IFC.1(2)		APP	None	
FDP_IFC.1(3)*		TFF	None	

[18] The [IDSSPP] FAU_STG.2 component has been selected because it is hierarchical to the Firewall PPs' FAU_STG.1.

Functional Component		Source PP(s)	CC Operations Applied	
			Firewall PP	IDS PP
FDP_IFF.1(1)	Simple security attributes	APP	Refinement, assignment	
FDP_IFF.1(2)		APP	Refinement, assignment	
FDP_IFF.1(3)*		TFF	Assignment	
FDP_RIP.2	Full residual information protection	Both	Hierarchical[19]	
FDP_UCT.1	Basic data exchange confidentiality	VPN	Assignment, selection	
FDP_UIT.1	Data exchange integrity	VPN	Assignment, selection	
FIA_ATD.1	User attribute definition	All	Refinement, assignment	Refinement
FIA_UAU.1	Timing of authentication	IDS[20]		Assignment
FIA_UAU.5	Multiple authentication mechanisms	Both	Refinement	
FIA_UID.2	User identification before any action	Both	None	
FIA_USB.1	User-Subject Binding	Other	Assignment[21]	
FMT_MOF.1(1)	Management of security functions behavior	Both	None	
FMT_MOF.1(2)		Both	None	
FMT_MOF.1(3)		IDS		Refinement
FMT_MOF.1(4)		Other	Selection, assignment	
FMT_MOF.1(5)		Other	Selection, assignment	
FMT_MSA.1(1)	Management of security	Both	Refinement*	

[19] FDP_RIP.2, hierarchical to FDP_RIP.1, is equivalent to the SFR erroneously identified in [APP-PP] as FDP_RIP.1. The [TFF-PP] included a less-inclusive FDP_RIP.1 requirement. The [APP-PP] requirement has been included in this ST.

[20] FIA_UAU.1 is specified here as being drawn from [IDSSPP] because it is missing in the requirements of [APP-PP] and [TFF-PP]. However, note that it is a dependency of FIA_AFL.1 which appears in both PPs. FIA_UAU.5 is not hierarchical to FIA_UAU.1 – it describes what authentication mechanisms are required for authenticated services, whereas FIA_UAU.1 specifies what services need be authenticated. Note that FIA_UAU.1 appears twice in [APP-PP] (in FAU_GEN and in the security requirements rationale), indicating that its omission might have been unintended.

[21] FIA_USB.1 has been adapted to conform to [RI#137].

Functional Component		Source PP(s)	CC Operations Applied	
			Firewall PP	IDS PP
FMT_MSA.1(2)	attributes	APP	None	
FMT_MSA.1(3)		Both	Refinement*	
FMT_MSA.1(4)		APP	None	
FMT_MSA.1(5)		VPN	Assignment, selection	
FMT_MSA.3	Static attribute initialization	Both	Refinement*	
FMT_MTD.1(1)	Management of TSF data	Both	None	
FMT_MTD.1(2)		Both	Refinement	
FMT_MTD.1(3)		IDS		Assignment, Refinement
FMT_MTD.1(4)		Other	Selection, assignment	
FMT_SMF.1	Specification of Management Functions	DEP	Assignment	
FMT_SMR.1	Security roles	All	Refinement	Refinement
FPT_AMT.1	Abstract machine testing	Other	Selection	
FPT_ITT.1	Basic internal TSF data transfer protection	Other	Selection	
FPT_RVM.1	Non-bypassability of the TSP	All	None	None
FPT_SEP.1	TSF domain separation	All	None	None
FPT_STM.1	Reliable time stamps	All	None	None
FPT_TST.1	TSF testing	Other	Selection, assignment	
FTP_ITC.1	Inter-TSF trusted channel	VPN	Selection, assignment	
FTP_TRP.1	Trusted path	Other	Selection, assignment	
IDS_SDC(EXP).1	System Data Collection	IDS		Explicit, selection, assignment
IDS_ANL(EXP).1	Analyser analysis	IDS		Explicit, selection, assignment
IDS_RCT(EXP).1	Analyser react	IDS		Explicit, assignment

Functional Component		**Source PP(s)**	**CC Operations Applied**	
			Firewall PP	**IDS PP**
IDS_RDR(EXP).1	Restricted Data Review	IDS		Explicit, assignment refinement
IDS_STG(EXP).1	Guarantee of System Data Availability	IDS		Explicit, assignment, selection refinement
IDS_STG(EXP).2	Prevention of System data loss	IDS		Explicit, refinement, selection

5.1.1. Security Audit (FAU)

5.1.1.1. Audit data generation (FAU_GEN.1)

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;

c[22]) the events in Table 5-2.

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, 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, information specified in column three of Table 5-2.

Table 5-2 - Auditable Events

Functional Component	Auditable Event	Additional Audit Record Contents	Source
FAU_GEN.1	**Start-up and shutdown of audit functions**		**IDS**
FAU_GEN.1	**Access to the IDS System**		**IDS**
FAU_GEN.1	**Access to the TOE and System Data**	**Object IDS, Requested access**	**IDS**
FAU_SAA.3	**Enabling and disabling of any of the analysis mechanisms; automated responses performed by the tool**		**Other**
FAU_SAR.1	**Reading of information from the audit records**		**IDS**
FAU_SAR.2	**Unsuccessful attempts to read information from the audit records**		**IDS**
FAU_SEL.1	**All modifications to the audit**		**IDS**

[22] The level of audit is 'not specified' for [APP-PP] and [TFF-PP], and 'basic' for [IDSSPP]. [IDSSPP] provides a table summarizing the applicable auditable events for the PP, adding the requirement for auditing 'Access to the System and access to the TOE and System data'. Subsection b) of FAU_GEN.1.1 omitted as described in Part 2 Annex C for the ‘not specified’ level of audit: “if ‘not specified’ is selected, the PP/ST author should fill in all desired auditable events in FAU_GEN.1.1c, and this part of the element (item b) can be removed entirely.”

The assignment of *other specifically defined auditable events* made in [IDSSPP]: "**Access to the System and access to the TOE and System data**" is specified by the FAU_GEN.1 entries in Table 5-2.

Functional Component	Auditable Event	Additional Audit Record Contents	Source
	configuration that occur while the audit collections functions are operating		
FAU_STG.3	**Actions taken due to exceeding of a threshold.**		**Other**
FAU_STG.4	**Actions taken due to the audit storage failure**		**Other**
FCS_COP.1	**Success and failure, and the type of cryptographic operation**	**The identity of the external IT entity attempting to perform the cryptographic operation.**	**Both**
FIA_UAU.1	**Any use of the authentication mechanism.**	**The user identities provided to the TOE, location.**	**All**[23]
FIA_UAU.5	**The final decision on authentication.**	**The user identity and the success or failure of the authentication.**	**APP**
FIA_UID.2	**All use of the user identification mechanism.**	**The user identities provided to the TOE, location.**	**All**
FIA_USB.1	**Success and failure of binding of user security attributes to a subject (e.g. success or failure to create a subject).**		**Other**
FDP_IFF.1	**All decisions on requests for information flow.**	**The presumed addresses of the source and destination subject.**	**Both**
FDP_UCT.1	**All VPN security association establishments.**	**The identity of the VPN peer.**	**VPN**
FDP_UIT.1	**All VPN security association establishments.**	**The identity of the VPN peer.**	**VPN**
FMT_MOF.1	**Use of the functions listed in this requirement pertaining to audit.**	**The identity of the authorized administrator performing the operation.**	**Both**
	All modifications in the behavior of the functions of the TSF.		**IDS**

[23] The audit requirement corresponding to FIA_UAU.1 appears in [TFF-PP] under FIA_UAU.5; however, the intent is the same in both PPs. The requirement for recording location is drawn from [IDSSPP].

Functional Component	Auditable Event	Additional Audit Record Contents	Source
FMT_MSA.3	**Modifications of the default setting of permissive or restrictive rules.** **All modifications of the initial value of security attributes.**		**Other**
FMT_MTD.1	**All modifications to the values of TSF data**		**IDS**
FMT_SMF.1	**Use of the management functions.**		**DEP**
FMT_SMR.1	**Modifications to the group of users that are part of the authorized administrator role.**	**The identity of the authorized administrator performing the modification and the user identity being associated with the authorized administrator role.**	**All**
	Unsuccessful attempts to authenticate the authorized administrator role.	**The user identity and the role.**	**APP**
FPT_AMT.1	**Execution of the tests of the underlying machine.**	**the results of the tests.**	**Other**
FPT_TST.1	**Execution of the TSF self tests and the results of the tests.**		**Other**
FPT_STM.1	**None[24].**		**Both**
FTP_ITC.1	**All attempted uses of the trusted channel functions.**	**Identification of the initiator and target of all trusted channel functions.**	**VPN**
FTP_TRP.1	**All attempted uses of the trusted path functions**	**Identification of the user associated with all trusted path invocations, if available.**	**Other**

[24] FMT_MTD.1(2) has been refined to restrict the setting of the time and date to no user in the operational environment of the TOE,; as a consequence, there is no requirement to audit an administrator change of the time and date used to form the timestamps in FPT_STM.1.1.

5.1.1.2. User identity association (FAU_GEN.2)

FAU_GEN.2.1 The TSF shall be able to associate each auditable event with the identity of the user that caused the event.

Application Note[25]: *There are some auditable events which may not be associated with a user, such as failed login attempts. It is acceptable that such events do not include a user identity.*

5.1.1.3. Simple attack heuristics (FAU_SAA.3)

FAU_SAA.3.1 The TSF shall be able to maintain an internal representation of the following signature events**: Stateful Inspection rules installed by an authorized administrator** that may indicate a violation of the TSP.

FAU_SAA.3.2 The TSF shall be able to compare the signature events against the record of system activity discernible from an examination of **network traffic mediated by the TOE**.

FAU_SAA.3.3 The TSF shall be able to indicate an imminent violation of the TSP when a system event is found to match a signature event that indicates a potential violation of the TSP.

Application Note: *this component is introduced to support IDS_ANL(EXP).1*.

5.1.1.4. Audit review (FAU_SAR.1)

FAU_SAR.1.1 The TSF shall provide an authorized administrator **and an authorized audit administrator** with the capability to read all audit trail data 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.

5.1.1.5. Restricted audit review (FAU_SAR.2)

FAU_SAR.2.1 The TSF shall prohibit all users read access to the audit records, except those users that have been granted explicit read-access.

5.1.1.6. Selectable audit review (FAU_SAR.3)

FAU_SAR.3.1 The TSF shall provide the ability to perform searches and sorting of audit data based on[26]:

a) user identity;

b) presumed subject address;

c) ranges of dates;

[25] This FAU_GEN.2 application note is derived from the corresponding [CAPP] requirement. This interpretation of FAU_GEN.2 is also compatible with that given in [I-0410].

[26] This requirement is inclusive of the corresponding requirements in [APP-PP], [TFF-PP] and [IDSSPP]. Specifically, the Firewall PPs require searches and sorting, whereas the [IDSSPP] requires only sorting. [APP-PP] requires a) through e), [TFF-PP] requires b) through e) and [IDSSPP] requires a), c), d), f) and g).

d) ranges of times;

e) ranges of addresses;

f) type of event; and

g) success or failure of related event.

5.1.1.7. Selective audit (FAU_SEL.1)

FAU_SEL.1.1 The TSF shall be able to include or exclude auditable events from the set of audited events based on the following attributes:

a) event type.

5.1.1.8. Guarantees of audit trail availability (FAU_STG.2)

FAU_STG.2.1 The TSF shall protect the stored audit records from unauthorized deletion.

FAU_STG.2.2 The TSF shall be able to prevent unauthorized modifications to the audit records **in the audit trail**[27].

FAU_STG.2.3 The TSF shall ensure that **all stored**[28] audit records will be maintained when the following conditions occur: audit storage exhaustion, failure and/or attack.

5.1.1.9. Action in case of possible audit data loss (FAU_STG.3)

FAU_STG.3.1 The TSF shall **send**[29] **an alarm** if the audit trail exceeds **a limit defined by the authorized administrator such that the amount of free disk space falls below a threshold defined by the administrator**.

5.1.1.10. Prevention of audit data loss (FAU_STG.4)

FAU_STG.4.1 The TSF shall prevent auditable events, except those taken by the authorized administrator and shall limit the number of audit records lost **and send an alarm** if the audit trail is full.

5.1.2. Cryptographic support (FCS)

5.1.2.1. Cryptographic key distribution (FCS_CKM.2(1))

FCS_CKM.2.1(1) The TSF shall distribute cryptographic keys **for IPSec VPNs and authentication of external IT entities** in accordance with a specified cryptographic key distribution

[27] In FAU_STG.2.2, the selection is given as 'prevent' from the Firewall PPs as it is stronger than 'detect' given in [IDSSPP]. The component has been updated to conform with the CCv2.2 syntax. This is consistent with [I-0422].

[28] See section 6.1.4.4 for an analysis of the maximum amount of audit data that can be expected to be lost in the event of audit storage failure, exhaustion, and/or attack, as required in the application note in [APP-PP] paragraph 91.

[29] Refinement: the word 'take' from the original Part 2 requirement has been omitted for clarity.

method **IKE** that meets the following: **RFC 2409 as constrained by NIAP PD-0105, with the following instantiation:**

a) Phase 1, the establishment of a secure authenticated channel between the TOE and another remote VPN endpoint, shall be performed using Main Mode;

b) The Diffie-Hellman key exchange[30] shall include the private group 14, 2048-bit MOD P;

c) SHA-1 is used exclusively as the pseudorandom function;

d) Quick Mode shall be able to generate key material that provides perfect forward secrecy;

e) All random values used for IKE shall be randomly generated using FIPS-approved random number generator;

f) The TSF shall be capable of authenticating IKE Phase 1 using the following methods as configured by the security administrator:

- **Authentication with digital signatures: The TSF shall use RSA;**
- **X.509v3 implementations shall be capable of checking for validity of the certificate path, and at option of the authorized administrator, check for certificate revocation; and**
- **Authentication with a pre-shared key: The TSF shall allow authentication using a pre-shared key.**

5.1.2.2. Cryptographic key distribution (FCS_CKM.2(2))

FCS_CKM.2.1(2) The TSF shall distribute cryptographic keys **for SIC and SSL VPNs** in accordance with a specified cryptographic key distribution method **TLS v1.0** that meets the following: **RFC 2246**.

5.1.2.3. Cryptographic operation (FCS_COP.1(1))

FCS_COP.1.1(1) The TSF shall perform encryption of remote authorized administrator sessions in accordance with a specified cryptographic algorithm: Triple Data Encryption Standard (DES) as specified in FIPS PUB 46-3 and implementing any mode of operation specified in FIPS PUB 46-3 with Keying Option 1 (K1, K2, K3 are independent keys) and cryptographic key sizes that are 192 binary digits in length that meet the following: FIPS PUB 46-3 with Keying Option 1 and FIPS PUB 140-1 (Level 1)[31].

[30] The Diffie Hellman key exchange is defined in RFC 2409 for IKE phase 1 IKE SA negotiation and for phase 2 IPSec SA negotiation when PFS is used. New Group Mode support is optional (and is not supported by the TOE).

[31] [APP-PP] and [TFF-PP] require the associated cryptographic module must comply at a minimum with FIPS PUB 140-1 Level 1. The cryptographic module for this TOE has been evaluated to FIPS PUB 140-2 Level 1.

5.1.2.4. Cryptographic operation (FCS_COP.1(2))

FCS_COP.1.1(2) The TSF shall perform **encryption and decryption of SIC and SSL VPN traffic** in accordance with a specified cryptographic algorithm: **Triple Data Encryption Standard (DES)** and cryptographic key sizes **that are 192 binary digits in length** that meet the following: **FIPS PUB 46-3**.

5.1.2.5. Cryptographic operation (FCS_COP.1(3))

FCS_COP.1.1(3) The TSF shall perform **encryption and decryption of IPSec VPN traffic** in accordance with specified cryptographic algorithms: **Triple Data Encryption Standard (DES); or Advanced Encryption Standard (AES)** and cryptographic key sizes **that are 192 binary digits in length for Triple DES; or 128 or 256 binary digits in length for AES** that meet the following: (**FIPS PUB 197 in CBC mode for AES; or FIPS PUB 46-3 with Keying Option 1 (K1, K2, K3 are independent keys) for Triple DES), RFC 2406 (Encapsulating Security Payload (ESP)) and FIPS PUB 140-2 (Level 1)**.

5.1.2.6. Cryptographic operation (FCS_COP.1(4))

FCS_COP.1.1(4) The TSF shall perform **production of Message Authentication Codes (MAC)** in accordance with a specified cryptographic algorithm: **HMAC-SHA-1** and cryptographic key sizes **that are 160 binary digits in length** that meet the following: **RFC 2104, FIPS PUB 198, RFC 2404 (The Use of HMAC-SHA-1-96 within ESP and AH) and FIPS PUB 140-2 (Level 1)**.

5.1.2.7. Cryptographic operation (FCS_COP.1(5))

FCS_COP.1.1(5) The TSF shall perform **secure hash computation** in accordance with a specified cryptographic algorithm: **SHA-1** and cryptographic key sizes **not applicable** that meet the following: **FIPS PUB 180-2 and FIPS PUB 140-2 (Level 1)**.

5.1.2.8. Cryptographic operation (FCS_COP.1(6))

FCS_COP.1.1(6) The TSF shall perform **authentication with digital signatures** in accordance with a specified cryptographic algorithm: **RSA** and cryptographic key sizes **1024, 2048 or 4096 binary digits in length** that meet the following: **PKCS #1**.

5.1.2.9. Cryptographic operation (FCS_COP.1(7))

FCS_COP.1.1(7) The TSF shall perform **IKE** in accordance with a specified cryptographic algorithm: **Diffie-Hellman** and cryptographic key sizes **768, 1024, 1536, 2048, 3072, 4096, 6144 or 8192 binary digits in length (for Diffie Hellman groups 1, 2, 5, 14, 15, 16, 17 and 18, respectively)** that meet the following: **RFC 2409 and FIPS PUB 140-2 (Level 1)**.

5.1.3. User data protection (FDP)

5.1.3.1. Subset information flow control (FDP_IFC.1(1))

FDP_IFC.1.1(1) The TSF shall enforce the UNAUTHENTICATED SFP on:

a) subjects: unauthenticated external IT entities that send and receive information through the TOE to one another;

b) information: **HTTP and SMTP** traffic sent through the TOE from one subject to another; and

c) operation: pass information **via unauthenticated application-level proxy**.

5.1.3.2. Subset information flow control (FDP_IFC.1(2))

FDP_IFC.1.1(2) The TSF shall enforce the AUTHENTICATED SFP on:

a) subjects: a human user or external IT entity that sends and receives FTP and Telnet information through the TOE to one another, only after the human user initiating the information flow has authenticated at the TOE per FIA_UAU.5;

b) information: FTP and Telnet traffic sent through the TOE from one subject to another; and

c) operation: initiate service and pass information.

5.1.3.3. Subset information flow control (FDP_IFC.1(3))

FDP_IFC.1.1(3) The TSF shall enforce the TRAFFIC FILTER SFP on:

a) subjects: unauthenticated external IT entities that send and receive information through the TOE to one another;

b) information: traffic sent through the TOE from one subject to another; and

c) operation: pass information.

Application Note: *the TRAFFIC FILTER SFP as defined covers all information flowing through the TOE, including information that is also controlled by the AUTHENTICATED and UNAUTHENTICATED SFPs.*

5.1.3.4. Simple security attributes (FDP_IFF.1(1)[32])

FDP_IFF.1.1(1) The TSF shall enforce the UNAUTHENTICATED SFP based on at least the following types of subject and information security attributes:

a) subject security attributes:

- presumed address;

b) information security attributes:

- presumed address of source subject;
- presumed address of destination subject;
- transport layer protocol;
- TOE interface on which traffic arrives and departs;
- service; and
- **date and time of information flow event**.

FDP_IFF.1.2(1) The TSF shall permit an information flow between a controlled subject and another controlled subject via a controlled operation if the following rules hold:

a) Subjects on an internal network can cause information to flow through the TOE to another connected network if[33]:

- all the information security attribute values are unambiguously permitted by the information flow security policy rules, where such rules may be composed from all possible combinations of the values of the information flow security attributes, created by the authorized administrator;
- the presumed address of the source subject, in the information, translates to an internal network address; and
- the presumed address of the destination subject, in the information, translates to an address on the other connected network.

b) Subjects on the external network can cause information to flow through the TOE to another connected network if:

- all the information security attribute values are unambiguously permitted by the information flow security policy rules, where such rules may be composed from all possible combinations of the values

[32] The complete set of functional elements of a component must be selected for inclusion in a PP. However, since the following functional elements from the FDP_IFF.1(1) component do not add anything significant to the PP, they have been moved here to allow for a clearer, smoother flowing presentation of FDP_IFF.1(1).

FDP_IFF.1.3 - The TSF shall enforce the [none].

FDP_IFF.1.4 - The TSF shall provide the following [none].

FDP-IFF.1.5 - The TSF shall explicitly authorize an information flow based on the following rules: [none].

[33] In [APP-PP], FDP_IFF.1.2 was incorrectly conditioned on the human user initiating the information flow having authenticated according to FIA_UAU.5. This has been corrected by [PD-0026].

of the information flow security attributes, created by the authorized administrator;

- the presumed address of the source subject, in the information, translates to an external network address; and
- the presumed address of the destination subject, in the information, translates to an address on the other connected network.

FDP_IFF.1.6(1) The TSF shall explicitly deny an information flow based on the following rules:

a) The TOE shall reject requests for access or services where the information arrives on an external TOE interface, and the presumed address of the source subject is an external IT entity on an internal network;

b) The TOE shall reject requests for access or services where the information arrives on an internal TOE interface, and the presumed address of the source subject is an external IT entity on the external network;

c) The TOE shall reject requests for access or services where the information arrives on either an internal or external TOE interface, and the presumed address of the source subject is an external IT entity on a broadcast network;

d) The TOE shall reject requests for access or services where the information arrives on either an internal or external TOE interface, and the presumed address of the source subject is an external IT entity on **a** loopback **address**[34];

e) The TOE shall reject requests in which the subject specifies the route in which information shall flow en route to the receiving subject; and

f) For **HTTP and SMTP**, the TOE shall deny any access or service requests that do not conform to its associated published protocol specification (e.g., RFC). This shall be accomplished through protocol filtering proxies that are designed for that purpose.

[34] The term "loopback address" is used in place of the original term "loopback network", per the guidance given in [PD-0018]. IPv4 treats any IP address with a network ID of 127 as a loopback address.

5.1.3.5. Simple security attributes (FDP_IFF.1(2) [35])

FDP_IFF.1.1(2) The TSF shall enforce the AUTHENTICATED SFP based on at least the following types of subject and information security attributes:

a) subject security attributes:

- presumed address; and
- **authenticated user identity**;

b) information security attributes:

- user identity;
- presumed address of source subject;
- presumed address of destination subject;
- transport layer protocol;
- TOE interface on which traffic arrives and departs;
- service (i.e., FTP and Telnet);
- security-relevant service command; and
- **date and time of information flow event**.

FDP_IFF.1.2(2) The TSF shall permit an information flow between a controlled subject and another controlled subject via a controlled operation if the following rules hold:

a) Subjects on an internal network can cause information to flow through the TOE to another connected network if:

- the human user initiating the information flow authenticates according to FIA_UAU.5 **and FIA_UAU.5(Env)**;
- all the information security attribute values are unambiguously permitted by the information flow security policy rules, where such rules may be composed from all possible combinations of the values of the information flow security attributes, created by the authorized administrator;
- the presumed address of the source subject, in the information, translates to an internal network address; and
- the presumed address of the destination subject, in the information, translates to an address on the other connected network.

---

[35] The complete set of functional elements of a component must be selected for inclusion in a PP. However, since the following functional elements from the FDP_IFF.1(2) component do not add anything significant to the PP, they have been moved here to allow for a clearer, smoother flowing presentation of FDP_IFF.1(2)

FDP_IFF.1.3 - The TSF shall enforce the [none].

FDP_IFF.1.4 - The TSF shall provide the following [none].

FDP-IFF.1.5 - The TSF shall explicitly authorize an information flow based on the following rules: [none].

b) subjects on the external network can cause information to flow through the TOE to another connected network if:

- the human user initiating the information flow authenticates according to FIA_UAU.5 **and FIA_UAU.5(Env)**;
- all the information security attribute values are unambiguously permitted by the information flow security policy rules, where such rules may be composed from all possible combinations of the values of the information flow security attributes, created by the authorized administrator;
- the presumed address of the source subject, in the information, translates to an external network address; and
- the presumed address of the destination subject, in the information, translates to an address on the other connected network.

FDP_IFF.1.6(2) The TSF shall explicitly deny an information flow based on the following rules:

a) The TOE shall reject requests for access or services where the information arrives on an external TOE interface, and the presumed address of the source subject is an external IT entity on an internal network;

b) The TOE shall reject requests for access or services where the information arrives on an internal TOE interface, and the presumed address of the source subject is an external IT entity on the external network;

c) The TOE shall reject requests for access or services where the information arrives on either an internal or external TOE interface, and the presumed address of the source subject is an external IT entity on a broadcast network;

d) The TOE shall reject requests for access or services where the information arrives on either an internal or external TOE interface, and the presumed address of the source subject is an external IT entity on **a** loopback **address**[36];

e) The TOE shall reject requests in which the subject specifies the route in which information shall flow en route to the receiving subject; and

f) The TOE shall reject Telnet or FTP command requests that do not conform to generally accepted published protocol definitions (e.g., RFCs). This must be accomplished through protocol filtering proxies designed for that purpose.

[36] The term "loopback address" is used in place of the original term "loopback network", per the guidance given in [PD-0018]. IPv4 treats any IP address with a network ID of 127 as a loopback address.

5.1.3.6. Simple security attributes (FDP_IFF.1(3)[37])

FDP_IFF.1.1(3) The TSF shall enforce the TRAFFIC FILTER SFP based on at least the following types of subject and information security attributes:

a) subject security attributes:

- presumed address;

b) information security attributes:

- presumed address of source subject;
- presumed address of destination subject;
- transport layer protocol;
- TOE interface on which traffic arrives and departs;
- service;
- **VPN community on which traffic arrives or departs, if any; and**
- **date and time of information flow event**.

FDP_IFF.1.2(3) The TSF shall permit an information flow between a controlled subject and another controlled subject via a controlled operation if the following rules hold:

a) Subjects on an internal network can cause information to flow through the TOE to another connected network if:

- all the information security attribute values are unambiguously permitted by the information flow security policy rules, where such rules may be composed from all possible combinations of the values of the information flow security attributes, created by the authorized administrator;
- the presumed address of the source subject, in the information, translates to an internal network address; and
- the presumed address of the destination subject, in the information, translates to an address on the other connected network.

b) Subjects on the external network can cause information to flow through the TOE to another connected network if:

- all the information security attribute values are unambiguously permitted by the information flow security policy rules, where such rules may be composed from all possible combinations of the values of the information flow security attributes, created by the authorized administrator;

---

[37] The complete set of functional elements of a component must be selected for inclusion in a PP. However, since the following functional elements from the FDP_IFF.1(3) component do not add anything significant to the PP, they have been moved here to allow for a clearer, smoother flowing presentation of FDP_IFF.1(3).

FDP_IFF.1.4 - The TSF shall provide the following [none].

FDP-IFF.1.5 - The TSF shall explicitly authorize an information flow based on the following rules: [none].

- the presumed address of the source subject, in the information, translates to an external network address; and
- the presumed address of the destination subject, in the information, translates to an address on the other connected network.

FDP_IFF.1.3(3) The TSF shall enforce the **following additional information flow control SFP rules:**

a) incoming IPSec or SSL VPN-encapsulated traffic shall be decrypted and verified in accordance with FDP_UCT.1 and FDP_UIT.1, based on VPN security attributes established by the authorized administrator for the VPN community that contains both the decrypting VPN gateway and the presumed VPN peer;

b) outgoing traffic shall be tunneled using IKE/IPSec or TLS in accordance with FDP_UCT.1 and FDP_UIT.1 to the VPN peer corresponding to the presumed address of the destination subject, based on VPN security attributes established by the authorized administrator for the VPN community that contains both the encrypting VPN gateway and the VPN peer; and

c) the incoming or outgoing traffic shall be associated with said VPN community, in the context of the enforcement of FDP_IFF.1.1(3) b).

FDP_IFF.1.6(3) The TSF shall explicitly deny an information flow based on the following rules:

a) The TOE shall reject requests for access or services where the information arrives on an external TOE interface, and the presumed address of the source subject is an external IT entity on an internal network;

b) The TOE shall reject requests for access or services where the information arrives on an internal TOE interface, and the presumed address of the source subject is an external IT entity on the external network;

c) The TOE shall reject requests for access or services where the information arrives on either an internal or external TOE interface, and the presumed address of the source subject is an external IT entity on a broadcast network; and

d) The TOE shall reject requests for access or services where the information arrives on either an internal or external TOE interface, and the presumed address of the source subject is an external IT entity on **a** loopback **address**[38].

Application Note: The TOE can make no claim as to the real address of any source or destination subject, therefore the TOE can only suppose that these addresses are accurate. Therefore, a "presumed address" is used to identify source and destination addresses. A "service", listed in FDP_IFF.1.1(3) subsection b), could be identified, for example, by a source port number and/or destination port number.

[38] The term "loopback address" is used in place of the original term "loopback network", per the guidance given in [PD-0018]. IPv4 treats any IP address with a network ID of 127 as a loopback address.

5.1.3.7. Subset residual information protection (FDP_RIP.2)

FDP_RIP.2.1 The TSF shall ensure that any previous information content of a resource is made unavailable upon the allocation of the resource to all objects[39].

5.1.3.8. Basic data exchange confidentiality (FDP_UCT.1)

FDP_UCT.1.1 The TSF shall enforce the **TRAFFIC FILTER SFP** to be able to transmit and receive objects in a manner protected from unauthorised disclosure.

5.1.3.9. Data exchange integrity (FDP_UIT.1)

FDP_UIT.1.1 The TSF shall enforce the **TRAFFIC FILTER SFP** to be able to transmit and receive user data in a manner protected from modification, deletion, insertion and replay errors.

FDP_UIT.1.2 The TSF shall be able to determine on receipt of user data, whether modification, deletion, insertion or replay has occurred.

[39] The wording in [TFF-PP] and [APP-PP] is slightly different regarding FDP_RIP.1. The former specifies that the objects in question are "resources that are used by the subjects of the TOE to communicate through the TOE to other subjects", whereas the latter simply refers to "all objects". Both PPs contain the same application note, giving a packet as an example. The more inclusive "all objects" phrasing was used in this ST. As this phrasing is then equivalent to the hierarchical FDP_RIP.2 [CC] Part 2 requirement, FDP_RIP.2 was included in this ST.

5.1.4. Identification and authentication (FIA)

5.1.4.1. User attribute definition (FIA_ATD.1)

FIA_ATD.1.1 The TSF shall maintain the following list of security attributes belonging to individual users:

a) identity;

b) association of a human user with **an** authorized administrator role[40];

c) authentication data; and

d) membership in user groups.

5.1.4.2. Timing of authentication (FIA_UAU.1)

FIA_UAU.1.1 The TSF shall allow **the following actions** on behalf of the user to be performed before the user is authenticated:

a) ICMP;

b) ARP;

c) Check Point RDP[41];

d) Download of the SSL Extender client from the TOE;

e) the information flows specified by UNAUTHENTICATED SFP and TRAFFIC FILTER SFP; and

f) information flows specified by AUTHENTICATED SFP that are authenticated with the support of the IT environment in accordance with FIA_UAU.5 and FIA_UAU.5(Env).

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.

Application Note:

Unauthenticated ICMP traffic to the TOE is allowed here to support a commonly used service. The administrator may disable this service altogether, or control access at the level of ICMP message type and code as specified in RFC 792. This is consistent with other U.S. Government Protection Profiles.

---

[40] For [IDSSPP], FIA_ATD.1 requires the TSF maintain: User identity, Authentication data, and Authorisations. An application note explains that at a minimum, there must be sufficient user information for I&A purposes, including any authorizations a user may possess. This ST uses the Firewall PP syntax; the requirement as stated meets the intent of the [IDSSPP]. In particular, authorization data in the context of this ST consists of the association with an authorized administrator role. The Firewall PP syntax was refined to allow multiple roles, as in [IDSSPP]. Membership in user groups has been added as a security attribute for consistency with FIA_USB.1, which has been derived from [CAPP].

[41] Check Point RDP is a proprietary unauthenticated UDP-based protocol (on port 259) used for VPN gateway discovery. It is not conformant with RDP as specified in RFC 908/1151.

ARP requests to the TOE are answered by the operating system of the TOE. The TOE also generates ARP responses on behalf of hosts for which Network Address Translation (NAT) is performed by the TOE.

RDP traffic to the TOE is allowed here to support dynamic discovery of peer IPSec gateways. The administrator may disable this service altogether.

The SSL Extender client can be downloaded from the TOE over an unauthenticated TLS channel, to allow a remote access VPN user to identify and authenticate to the TOE using SSL VPN.

5.1.4.3. Multiple authentication mechanisms (FIA_UAU.5)

FIA_UAU.5.1 The TSF shall provide single-use[42] authentication mechanisms to support user authentication.

FIA_UAU.5.2 The TSF shall authenticate any user's claimed identity according to the following multiple authentication mechanism rules:

a) **SIC certificate-based** authentication mechanism shall be used for authorized administrators to access the TOE remotely such that successful authentication must be achieved before allowing any other TSF-mediated actions on behalf of that authorized administrator;

b) **IKE -based authentication mechanism or** single-use **authenticator-based** authentication mechanism shall be used for authorized external IT entities accessing the TOE such that successful authentication must be achieved before allowing any other TSF-mediated actions on behalf of that authorized external IT entity;

c) **IKE or TLS-based authentication mechanism or** single-use **password** authentication mechanism shall be used for human users sending or receiving information through the TOE using FTP or Telnet or other protocols as configured by a authorized administrator such that successful authentication must be achieved before allowing any other TSF-mediated actions on behalf of that human user.

Application Note: *This SFR was refined to be more explicit on what authentication mechanisms are used in each of the FIA_UAU.5.2 scenarios.*

Administrators are authenticated by the TSF using SIC (TLS) certificate-based authentication.

IKE authentication for authorized external IT entities accessing the TOE can be performed using either signature or shared-secret authentication. Alternatively, authorized external IT entities may be authenticated using single-use authenticators.

IKE or TLS authentication for human users sending information through the TOE is to be provided via the TOE's Remote Access VPN functionality.

[42] Re-usable passwords are not presented in FIA_UAU.5.1 as a mechanism for user authentication. The PP reference to reusable password-based authentication has been omitted because only single-use authentication mechanisms (including single-use password and certificate-based authentication) are used in the evaluated configuration.

Where single-use password authentication is configured by the authorized administrator, the TSF authenticates human users sending information through the TOE with the support of the IT environment: the TSF identifies the user and requests a single-use password; the password is sent to an external authentication server for identity verification. This is consistent with NIAP precedent decision [PD-0115]. Required IT environment support for authentication is specified in FIA_UAU.5(Env).

5.1.4.4. User identification before any action (FIA_UID.2)

FIA_UID.2.1 The TSF shall require each user to identify itself before allowing any other TSF-mediated actions on behalf of that user.

Application Note: *All users, whether authenticated or not, will always be identified at least by a source network identifier.*

5.1.4.5. User-subject binding (FIA_USB.1)[43]

FIA_USB.1.1 The TSF shall associate the following user security attributes with subjects acting on the behalf of that user:

a) The user identity which is associated with auditable events;

b) The user identity or identities which are used to enforce all SFPs;

c) The group membership or memberships used to enforce all SFPs.

FIA_USB.1.2 The TSF shall enforce the following rules on the initial association of user security attributes with subjects acting on the behalf of users:

a) The identity for an authenticated user associated with an authorized administrator role is established in the process of performing the administrator login to the Management GUIs;

b) All users sending information through the TOE are initially identified by the presumed source network identifier;

c) The identity for users sending information through the TOE over a Remote Access VPN is established from the identity transferred as part of the IKE or TLS protocols;

d) A subject acting on behalf of a human user sending information through the TOE according to the AUTHENTICATED SFP that authenticates the user using a single-use password will be associated with the user's authenticated identity;

e) Group memberships are associated with a subject acting on behalf of the user in accordance with the security attributes corresponding to the user identity in accordance with FIA_ATD.1.

FIA_USB.1.3 The TSF shall enforce the following rules governing changes to the user security attributes associated with subjects acting on the behalf of users: **none**.

[43] FIA_USB.1 was adapted from the corresponding [CAPP] requirement.

5.1.5. Security Management (FMT)

5.1.5.1. Management of security functions behaviour (FMT_MOF.1(1))

FMT_MOF.1.1(1) The TSF shall restrict the ability to enable, disable the functions:

a) operation of the TOE; and

b) multiple use authentications as described in FIA_UAU.5

to an authorized administrator.

Application Note: By "Operation of the TOE" in a) above, the PP authors refer to having the TOE start up (enable operation) and shut down (disable operation). By "multiple use" in b) above, the PPs refer to the management of password and single-use authentication mechanisms.

5.1.5.2. Management of security functions behaviour (FMT_MOF.1(2))

FMT_MOF.1.1(2) The TSF shall restrict the ability to enable, disable, determine and modify the behaviour of the functions:

a) audit trail management;

b) backup and restore for TSF data, information flow rules, and audit trail data; and

c) communication of authorized external IT entities with the TOE

to an authorized administrator.

Application Note: Determine and modify the behavior of element c (communication of authorized external IT entities with the TOE) is intended to cover functionality such as providing a range of addresses from which the authorized external entity can connect.

5.1.5.3. Management of security functions behaviour (FMT_MOF.1(3))

FMT_MOF.1.1(3) The TSF shall restrict the ability to modify the behaviour of the functions of **IDS** System data collection, analysis and reaction to authorized System administrators.

5.1.5.4. Management of security functions behaviour (FMT_MOF.1(4))

FMT_MOF.1.1(4) The TSF shall restrict the ability to enable, disable the functions **ICMP, Check Point RDP** to an authorized administrator.

5.1.5.5. Management of security functions behaviour (FMT_MOF.1(5))

FMT_MOF.1.1(5) The TSF shall restrict the ability to enable the functions **SIC** to an authorized administrator.

5.1.5.6. Management of security attributes (FMT_MSA.1(1))

FMT_MSA.1.1(1) The TSF shall enforce the UNAUTHENTICATED SFP **and TRAFFIC FILTER SFP** to restrict the ability to delete attributes from a rule, modify attributes in a rule, add attributes to a rule the security attributes listed in section FDP_IFF1.1(1) **and FDP_IFF.1(3), respectively** to the authorized administrator.

5.1.5.7. Management of security attributes (FMT_MSA.1(2))

FMT_MSA.1.1(2) The TSF shall enforce the AUTHENTICATED SFP to restrict the ability to delete attributes from a rule, modify attributes in a rule, add attributes to a rule the security attributes listed in section FDP_IFF1.1(2) to the authorized administrator.

5.1.5.8. Management of security attributes (FMT_MSA.1(3))

FMT_MSA.1.1(3) The TSF shall enforce the UNAUTHENTICATED SFP **and TRAFFIC FILTER SFP** to restrict the ability to delete and create the security attributes information flow rules described in FDP_IFF.1(1) **and FDP_IFF.1(3), respectively** to the authorized administrator.

5.1.5.9. Management of security attributes (FMT_MSA.1(4))

FMT_MSA.1.1(4) The TSF shall enforce the AUTHENTICATED SFP to restrict the ability to delete and create the security attributes information flow rules described in FDP_IFF.1(2) to the authorized administrator.

5.1.5.10. Management of security attributes (FMT_MSA.1(5))

FMT_MSA.1.1(5) The TSF shall enforce the **TRAFFIC FILTER SFP** to restrict the ability to create, query, modify and delete the security attributes **VPN rules** to **the authorized administrator**.

5.1.5.11. Static attribute initialization (FMT_MSA.3)

FMT_MSA.3.1 The TSF shall enforce the UNAUTHENTICATED SFP**, TRAFFIC FILTER SFP** and AUTHENTICATED SFP to provide restrictive default values for information flow security attributes that are used to enforce the SFP.

FMT_MSA.3.2 The TSF shall allow the authorized administrator to specify alternative initial values to override the default values when an object or information is created.

Application Note: The default values for the information flow control security attributes appearing in FDP_IFF.1 are intended to be restrictive in the sense that both inbound and outbound information is denied by the TOE until the default values are modified by an authorized administrator.

The evaluated configuration includes a set of restrictive implicit rules that allow authenticated management traffic to any defined SmartCenter Server hosts, authentication protocols to any defined authorized authentication servers in the IT environment, as well as VPN-related protocols.

5.1.5.12. Management of TSF data (FMT_MTD.1(1))

FMT_MTD.1.1(1) The TSF shall restrict the ability to query, modify, delete, and assign the user attributes defined in FIA_ATD.1.1 to the authorized administrator.

5.1.5.13. Management of TSF data (FMT_MTD.1(2))

FMT_MTD.1.1(2) The TSF shall restrict the ability to set the time and date used to form the timestamps in FPT_STM.1.1 to **no user in the operational environment of the TOE**[44].

5.1.5.14. Management of TSF data (FMT_MTD.1(3))

FMT_MTD.1.1(3) The TSF shall restrict the ability to query and add **IDS** System and audit data, and shall restrict the ability to query and modify all other TOE data to **the following roles defined in FMT_SMR.1: the authorized administrator may query and modify all TOE data, and the authorized audit administrator may query IDS System and audit data**.

5.1.5.15. Management of TSF data (FMT_MTD.1(4))

FMT_MTD.1.1(4) The TSF shall restrict the ability to clear, query or modify the **thresholds for the detection of an imminent audit storage failure and the actions taken** to **the authorized administrator**.

5.1.5.16. Specification of management functions (FMT_SMF.1)

FMT_SMF.1.1 The TSF shall be capable of performing the following security management functions: **as specified in Table 5-3 below.**

Table 5-3- Specification of Management Functions

Component	Management Function
FMT_MOF.1(1)	**Startup and shutdown of the TOE**
	Management of multiple authentication mechanisms
FMT_MOF.1(2)	**Audit trail management**
	Backup and restore for TSF data, information flow rules, and audit trail data
	Control of communication with authorized external IT entities

[44] The hardware clock is set during installation of the TOE. This provides reliable timestamps that meet the FPT_STM.1 requirement. Administrators do not modify the time and date after the TOE is operational. In order to synchronize between the TOE's clock and other IT entities' clocks, an authorized NTP server may be configured during installation of the TOE; this server serves as an external IT entity that is authorized to update the clock.

Component	Management Function
FMT_MOF.1(3)	**Modifying IDS System behaviour**
FMT_MOF.1(4)	**Enabling or disabling ICMP and Check Point RDP support**
FMT_MOF.1(5)	**Enabling SIC connectivity between management and appliance**
FMT_MSA.1(1), FMT_MSA.1(3)	**Management of unauthenticated information flow control rules**
FMT_MSA.1(2), FMT_MSA.1(4)	**Management of authenticated information flow control rules**
FMT_MSA.1(5)	**Management of VPN rules**
FMT_MSA.3	**Specification of alternative initial values to override the restrictive default values for information flow security attributes**
FMT_MTD.1(1)	**Management of user security attributes**
FMT_MTD.1(3)	**Management of TOE data and performing audit queries**
FMT_MTD.1(4)	**Management of the thresholds and actions taken in case of imminent audit storage failure**

5.1.5.17. Security roles (FMT_SMR.1)

FMT_SMR.1.1 The TSF shall maintain the following role**s:** authorized administrator**, authorized audit administrator**.

FMT_SMR.1.2 The TSF shall be able to associate human users with **roles**.

5.1.6. Protection of the TSF (FPT)

5.1.6.1. Abstract machine testing (FPT_AMT.1)

FPT_AMT.1.1	The TSF shall run a suite of tests during initial start-up to demonstrate the correct operation of the security assumptions provided by the abstract machine that underlies the TSF.

5.1.6.2. Basic internal TSF data transfer protection

FPT_ITT.1	The TSF shall protect TSF data from disclosure and modification when it is transmitted between separate parts of the TOE.

5.1.6.3. Non-bypassability of the TSP (FPT_RVM.1)

FPT_RVM.1.1	The TSF shall ensure that TSP enforcement functions are invoked and succeed before each function within the TSC is allowed to proceed.

5.1.6.4. TSF domain separation (FPT_SEP.1)

FPT_SEP.1.1	The TSF shall maintain a security domain for its own execution that protects it from interference and tampering by untrusted subjects.
FPT_SEP.1.2	The TSF shall enforce separation between the security domains of subjects in the TSC.

5.1.6.5. Reliable time stamps (FPT_STM.1)

FPT_STM.1.1	The TSF shall be able to provide reliable time stamps for its own use.

5.1.6.6. TSF Testing (FPT_TST.1)

FPT_TST.1.1	The TSF shall run a suite of tests during initial start-up and periodically during normal operation to demonstrate the correct operation of **the FIPS 140-2 cryptographic module and the operational status of critical processes**.
FPT_TST.1.2	The TSF shall provide authorized users with the capability to verify the integrity of **policy files**.
FPT_TST.1.3	The TSF shall provide authorized users with the capability to verify the integrity of stored TSF executable code.

5.1.7. Trusted path/channels (FTP)

5.1.7.1. Inter-TSF trusted channel (FTP_ITC.1)

FTP_ITC.1.1	The TSF shall provide a communication channel between itself and a remote trusted IT product that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.
FTP_ITC.1.2	The TSF shall permit the TSF[45] or the remote trusted IT product to initiate communication via the trusted channel.
FTP_ITC.1.3	The TSF shall initiate communication via the trusted channel for **VPN traffic and for communication with external authorized IT entities**.

5.1.7.2. Trusted Path (FTP_TRP.1)

FTP_TRP.1.1	The TSF shall provide a communication path between itself and local 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 local users to initiate communication via the trusted path.
FTP_TRP.1.3	The TSF shall require the use of the trusted path for **administration of the TOE**.

[45] The TSF can initiate IPSec VPN tunnels to an IPSec VPN peer; SSL VPN tunnels are always initiated by the remote trusted IT product (the remote access VPN client).

5.1.8. IDS Component Requirements (IDS)

5.1.8.1. Analyzer analysis (IDS_ANL(EXP).1)

IDS_ANL(EXP).1.1 The System shall perform the following analysis function(s) on all IDS data received: signature.

IDS_ANL(EXP).1.2 The System shall record within each analytical result at least the following information:

a) Date and time of the result, type of result, identification of data source.

5.1.8.2. Analyzer react (IDS_RCT(EXP).1)

IDS_RCT(EXP).1.1 The System shall send an alarm to **authorized administrators and authorized audit administrators** and take **action as configured by an authorized administrator: logging and/or dropping the suspected traffic** when an intrusion is detected.

5.1.8.3. Restricted Data Review (IDS_RDR(EXP).1)

IDS_RDR(EXP).1.1 The System shall provide **an authorized administrator and an authorized audit administrator** with the capability to read **all audit trail data** from the **IDS** System data.

IDS_RDR(EXP).1.2 The System shall provide the **IDS** System data in a manner suitable for the user to interpret the information.

IDS_RDR(EXP).1.3 The System shall prohibit all users read access to the **IDS** System data, except those users that have been granted explicit read-access.

5.1.8.4. System Data Collection (IDS_SDC(EXP).1)

IDS_SDC(EXP).1.1 The System shall be able to collect the following information from the targeted IT System resource(s):

a) service requests, network traffic, detected known vulnerabilities.

IDS_SDC(EXP).1.2 At a minimum, the System shall collect and record 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) The additional information specified in the Details column of Table 5-4.

Table 5-4 - System Events

Component	Event	Details
IDS_SDC.1	**Service Requests**	**Specific service, source address, destination address**
IDS_SDC.1	**Network traffic**	**Protocol, source address, destination address**
IDS_SDC.1	**Detected known vulnerabilities**	**Identification of the known vulnerability**

5.1.8.5. Guarantee of System Data Availability (IDS_STG(EXP).1)

IDS_STG(EXP).1.1 The System shall protect the stored **IDS** System data from unauthorized deletion.

IDS_STG(EXP).1.2 The System shall protect the stored **IDS** System data from modification.

Application Note: Authorized deletion of data is not considered a modification of IDS System data in this context. This requirement applies to the actual content of the IDS System data, which should be protected from any modifications.

IDS_STG(EXP).1.3 The System shall ensure that **all stored IDS** System data will be maintained when the following conditions occur: System data storage exhaustion, failure and/or attack.

5.1.8.6. Prevention of System data loss (IDS_STG(EXP).2)

IDS_STG(EXP).2.1 The System shall prevent **IDS** System data, except those taken by the authorized **administrator** and send an alarm if the storage capacity has been reached.

5.2. TOE Security Assurance Requirements

The security assurance requirements for the TOE are the Evaluation Assurance Level (EAL) 4 components defined in Part 3 of the Common Criteria ([CC]), augmented with the [CC] Part 3 component ALC_FLR.3.

Where an assurance requirement was drawn from one of the claimed PPs, it is identified in the 'Source PP(s)' column of Table 5-5, using the conventions described in section 5.1. Augmented requirements are denoted as AUGMEN.

No operations are applied to the assurance components. Where assurance requirements have been updated in CCv2.2 (AVA_VLA.3), the assurance requirements in this ST conform to those updated requirements, by reference.

Table 5-5- TOE Security Assurance Requirements

Assurance Class	Assurance Components		Source PP(s)
Configuration Management (ACM)	ACM_AUT.1	Partial CM automation	AUGMEN
	ACM_CAP.4	Generation support and acceptance procedures	AUGMEN
	ACM_SCP.2	Problem tracking CM coverage	AUGMEN
Delivery and Operation (ADO)	ADO_DEL.2	Detection of modification	AUGMEN
	ADO_IGS.1	Installation, generation, and start-up procedures	ALL
Development (ADV)	ADV_FSP.2	Fully defined external interfaces	APP
	ADV_HLD.2	Security enforcing high-level design	BOTH
	ADV_LLD.1	Descriptive low-level design	BOTH
	ADV_IMP.1	Subset of the implementation of the TSF	BOTH
	ADV_RCR.1	Informal correspondence demonstration	ALL
	ADV_SPM.1	Informal TOE security policy model	AUGMEN
Guidance Documents (AGD)	AGD_ADM.1	Administrator guidance	ALL
	AGD_USR.1	User guidance	ALL
Lifecycle	ALC_DVS.1	Identification of security measures	AUGMEN

Assurance Class	**Assurance Components**		**Source PP(s)**
support (ALC)	ALC_FLR.3	Systematic flaw remediation	AUGMEN
	ALC_LCD.1	Developer defined life-cycle model	AUGMEN
	ALC_TAT.1	Well-defined development tools	BOTH
Tests (ATE)	ATE_COV.2	Analysis of coverage	AUGMEN
	ATE_DPT.1	Testing: high-level design	AUGMEN
	ATE_FUN.1	Functional testing	ALL
	ATE_IND.2	Independent testing – sample	ALL
Vulnerability Assessment (AVA)	AVA_MSU.2	Validation of analysis	AUGMEN
	AVA_SOF.1	Strength of TOE security function evaluation	ALL
	AVA_VLA.2	Independent vulnerability analysis	ALL

5.3. Security Functional Requirements for the IT Environment

The following are security functional requirements for the IT environment, intended to specify what the IT environment must provide in order to meet the security objectives for the IT environment: OE.IDAUTH and OE.VPN.

5.3.1. User Data Protection (FDP)

5.3.1.1. Basic data exchange confidentiality (FDP_UCT.1(Env))

FDP_UCT.1.1(Env) The **IT Environment** shall enforce the **TRAFFIC FILTER SFP** to be able to transmit and receive objects in a manner protected from unauthorised disclosure.

5.3.1.2. Data exchange integrity (FDP_UIT.1(Env))

FDP_UIT.1.1(Env) The **IT Environment** shall enforce the **TRAFFIC FILTER SFP** to be able to transmit and receive user data in a manner protected from modification, deletion, insertion and replay errors.

FDP_UIT.1.2(Env) The **IT Environment** shall be able to determine on receipt of user data, whether modification, deletion, insertion or replay has occurred.

Application Note: *the FDP_UCT.1(Env) and FDP_UIT.1(Env) requirements for the IT environment are necessary because peer VPN gateways must implement corresponding security functions for the TOE to be able to provide adequate protection from disclosure and modification for VPN traffic.*

For example, a peer gateway that leaks symmetric keys will allow attackers to decipher encrypted information sent by the TOE to that gateway, and to maliciously modify information that is being sent to the TOE through the peer gateway, without the TOE being able to detect this modification.

5.3.2. Identification and Authentication (FIA)

5.3.2.1. Multiple authentication mechanisms (FIA_UAU.5(Env))

FIA_UAU.5.1(Env) The **IT Environment** shall provide single-use authentication mechanisms to support user authentication.

FIA_UAU.5.2(Env) The **IT Environment** shall **support the authentication of** any user's claimed identity according to the following multiple authentication mechanism rules:

a) If a single-use password authentication mechanism is to be used for human users sending or receiving information through the TOE, the IT environment shall provide an authentication server that validates single-use passwords for a given user identity, using the protocols: RADIUS or SecurID;

b) If an external Certificate Authority is to be used for VPN-based authentication of authorized external IT entities accessing the TOE or for hu-

man users sending or receiving information through the TOE, the IT environment shall provide the following authentication support:

1) **Certificates shall be generated and distributed by a trusted Certificate Authority (CA) that guarantees the binding between the certificate and associated authentication credentials, and the presumed identity of its holder, in a manner that is commensurate with the security environment of the TOE and the CA; and**

2) **Certificate revocation information shall be made available to the TOE, using the protocols: LDAP, HTTP or OCSP.**

Application Note: *this SFR for the IT environment was introduced in view of the guidance supplied by [PD-0115]. It is in direct support of the FIA_UAU.5 SFR for the TOE.*

5.3.3. Trusted path/channels (FTP)

5.3.3.1. Inter-TSF trusted channel (FTP_ITC.1(Env))

FTP_ITC.1.1(Env) The **IT Environment** shall provide a communication channel between itself and **the TSF** that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.

FTP_ITC.1.2(Env) The **IT Environment** shall permit the TSF or the remote trusted IT product to initiate communication via the trusted channel.

FTP_ITC.1.3(Env) The **IT Environment** shall initiate communication via the trusted channel for **VPN traffic to or through the TOE**.

6. TOE Summary Specification

This section describes the security functions of the TOE and the assurance measures taken to ensure correct implementation, and maps them to the security requirements.

6.1. TOE Security Functions

This section presents the IT security functions (SFs) and a mapping of security functions to security functional requirements. The TOE performs the following security functions:

- Stateful Inspection
- Security Servers
- VPN
- Audit
- Security Management
- SIC
- Identification and Authentication (I&A)
- TSF Protection

6.1.1. Stateful Inspection

6.1.1.1. Anti-Spoofing

When an IP packet is received on a network interface, its source address is compared to topology information configured by the authorized administrator. If the source address does not correspond to the set of network addresses that match the given network interface, the packet is dropped.

6.1.1.2. Packet Inspection

Every IPv4 packet received by the Check Point VPN-1 Power/UTM appliance is intercepted by the Stateful Inspection SF. A Virtual Machine (VM) matches the packet against rules encoded in a machine language-like declarative language named 'INSPECT'. INSPECT operators perform pattern matching on incoming packets, as a function of the firewall state tables (e.g. connection table), and trigger responses that include:

- Accept - the packet is allowed through;
- Drop – the packet is dropped without notification to the sender;
- Reject – the packet is dropped and the presumed sender is notified.

Packet pattern matching can be configured to have security-relevant side-effects that include updating firewall state tables, and generating log messages.

INSPECT rules may also be conditioned by current date and time.

6.1.1.3. Post-Inspect

Every IPv4 packet that is allowed by the Packet Inspection capability is fed through a second set of INSPECT rules that attempt to match the packet against sets of attack signatures that may be installed by an authorized administrator (SmartDefense Updates).

6.1.1.4. Residual Information Protection

When an incoming network frame is received by a Check Point VPN-1 Power/UTM appliance, it is written by the network interface controller into kernel message buffers. Each kernel buffer is associated with a separate header that keeps track of the number of bytes of data in the buffer. The kernel clears the header prior to reading new data, and the header is updated with the count of bytes transferred by the controller.

When the buffer resource is abstracted into a message object, the object is initialized to refer only to data that has actually been overwritten in the context of the current message. This ensures that any residual information that might remain in the kernel buffer resource from previous messages is made unavailable.

State information resources that are allocated as part of the packet processing are cleared before use.

All buffers containing cryptographic keying material are zeroed out before being deallocated, so that previous contents are made unavailable when allocating the buffer for any object.

6.1.1.5. Implied Rules

A set of predefined rules is implicitly incorporated in the information flow control policy. This set of rules can be tailored during TOE installation.

The implied rules in the evaluated configuration of the TOE are:

- Implicit drop rule: any packet that cannot be matched by a Stateful Inspection rule is dropped (with no logging);
- Connectivity queries to the TOE are allowed by default (but may be constrained by the authorized administrator);
- IP packets containing IP options are dropped by default (but may be selectively allowed by the authorized administrator).

6.1.1.6. SFR Mapping

The following SFRs are satisfied by the Stateful Inspection SF:

- **FAU_SAA.3** – network traffic mediated by the TOE is compared against signature events encoded in INSPECT language. Because INSPECT operators can be configured to modify state tables as a function of incoming packets, and because

pattern matching on incoming packets is a function of state table information, signature events can be configured to detect both simple single-packet and complex multi-packet events that may indicate an attempt to violate the TSP. Encoded signature events can be set to log the detected potential violation.

INSPECT matching is performed twice: by the Packet Inspection capability, and by the Post Inspect capability. An authorized administrator can set up IDS signature events using both capabilities; by setting up a Packet Inspection rule that matches the defined signature and reacts accordingly, or by loading a canned set of signature events that will be matched during Post Inspect.

- **FDP_IFC.1(1)**, **FDP_IFF.1(1)**, **FDP_IFC.1(2)**, **FDP_IFF.1(2)**, **FDP_IFC.1(3)** and **FDP_IFF.1(3)** – Packet Inspection is applied to all packets, including both packets that are only traffic-filtered, and packets that are redirected to a Security Server proxy. Packet Inspection ensures that information may flow through the TOE only if permitted by the Stateful Inspection rules created by the authorized administrator. The rules may be matched against the following security attributes:
    - Packet contents, including: presumed IP addresses of source and destination subjects, transport layer protocol and service (port);
    - TOE interface on which traffic arrives and departs, as determined by topology information that binds interfaces to valid source addresses, and static routing information that binds interfaces to relevant destination addresses;
    - Whether the traffic is encrypted and the associated VPN community (determined by the VPN-authenticated identity of the peer VPN gateway); and
    - Current date and time;

  Anti-Spoofing verifies that presumed source addresses match defined topology. In particular, information flow arriving on a network interface is denied where the presumed address of the source subject is an external IT entity on a broadcast network or on a loopback address.

  IP packets containing Source Route IP options are dropped by the default set of Implied Rules. TOE evaluation configuration guidance instructs administrators not to configure the TOE to allow these options that might be used to specify the route in which information shall flow en route to the receiving subject.

  Note: For FTP and Telnet traffic, TOE evaluated configuration guidance instructs the authorized administrator to require VPN-based authentication (via a condition accepting only FTP or Telnet traffic belonging to a Remote Access VPN community) if a User Authentication rule (see section 6.1.2.2 below) is not configured.

- **FDP_RIP.2** – this requirement is met by the Residual Information Protection capability.

- **FMT_MSA.3** – the implicit drop rule ensures that the default rule for information flow control is restrictive, being limited to the other Implied Rules. An authorized administrator can specify alternative rules that override these default values.
- **IDS_ANL(EXP).1** – signature analysis is performed on all traffic as described above for FAU_SAA.3.
- **IDS_RCT(EXP).1** – when an intrusion is detected, i.e. when incoming traffic matches an IDS signature encoded in INSPECT language, Packet Inspection can be configured to log the event and/or drop the suspected traffic.

6.1.2. Security Servers

6.1.2.1. General

Security Servers are proxy processes that can be run on the Check Point VPN-1 Power/UTM appliance. Security Servers are provided for the protocols: Telnet, FTP, HTTP and SMTP. When traffic that is associated with one of these protocols is received by the TOE, the TOE in its evaluated configuration is configured to redirect the traffic to be filtered by an appropriate Security Server. Security Servers validate access or service request for conformance to its associated published protocol specification, and may be configured to require user authentication.

6.1.2.2. FTP Security Server

The FTP Security Server validates FTP commands against a list of acceptable FTP commands that is a subset of the commands defined in [RFC0959]. The authorized administrator can configure the list of allowed and blocked commands. By default, all FTP commands are allowed except for REST, MACB, SITE, SOCK, and mail-related commands, which are always blocked. FTP response codes are also validated.

An authorized administrator can configure whether the GET or PUT commands are allowed for a defined FTP Server, and restrict access to specified paths and filenames.

The FTP Security Server performs a sanity validation for the PORT command parameter, preventing the use of a port that is reserved for a known defined service, or invalid string values.

6.1.2.3. Telnet Security Server

The Telnet Security Server validates Telnet option codes against a list of allowed option codes. In addition, the Echo Data option is suppressed by default.

6.1.2.4. HTTP Security Server

The HTTP Security Server provides the following validation checks for HTTP traffic:

Table 6-1- HTTP Security Server Protocol Validation

Validation	Default Values
Enforce maximum URL length	2048 bytes
Enforce maximum HTTP header length	2100 bytes
Enforce maximum number of HTTP headers	500
Reject URL with double slash, URI query, or non-standard scheme	Enabled: reject double slash
Reject request headers with non-ASCII characters	Enabled
Reject response headers with non-ASCII characters	Disabled
Reject requests and responses with an administrator-defined header name or header value	Defaults to preventing peer-to-peer traffic including: KaZaA, Gnutella and ICQ
Block HTTP requests with an administrator-defined HTTP method (e.g. GET and POST), URL, or scheme	None
Block partial range requests and responses	Enabled
Block content compression	Enabled

6.1.2.5. SMTP Security Server

The SMTP Security Server validates SMTP traffic, rejecting requests that do not conform to [RFC2821] specifications for MIME and message headers, for SMTP commands and for base64 decoding.

An authorized administrator can configure restrictions for attachment types and mail size.

6.1.2.6. User Authentication

Security servers may be configured to require the human user to authenticate using a single-use password mechanism, by forwarding the user's password to a remote authentication server in the IT environment, using the RADIUS or SecurID protocols. User Authentication is available for the protocols FTP, Telnet and HTTP.

Note: For FTP and Telnet traffic, TOE evaluated configuration guidance instructs the authorized administrator to require User Authentication for all traffic not belonging to a Remote Access VPN community (and therefore not IKE-authenticated).

6.1.2.7. SFR Mapping

The following SFRs are satisfied by the Security Servers SF:

- **FDP_IFC.1(1)** and **FDP_IFF.1(1)** – the requirement for protocol filtering proxies is met by the HTTP and SMTP Security Servers.

- **FDP_IFC.1(2)** and **FDP_IFF.1(2)** – the requirement for protocol filtering proxies is met by the FTP and Telnet Security Servers. User authentication requires the human user initiating the information flow to authenticate using a single-use authentication mechanism.

6.1.3. VPN

6.1.3.1. IPSec VPN

Traffic that has been defined as being tunneled over IPSec is handled as follows:

- An IPSec Security Association (SA) is established with the IPSec VPN peer, using the IKE protocol in accordance with RFC 2409:
  - IKE phase 1 is performed using Main Mode;
  - Authentication is performed via RSA signatures, or pre-shared keys;
  - PKCS#1 encoding is used for RSA. Key sizes of 1024, 2048 and 4096 bits are supported;
  - SHA-1 is used as the pseudo-random function;
  - HMAC-SHA-1 is used for authenticating the IKE key exchange;
  - Diffie Hellman groups supported include groups 1, 2, 5, 14, 15, 16, 17 and 18;
  - Perfect Forward Secrecy (PFS) can be optionally enabled for the exchange. KE payloads are used when PFS is specified;
  - All random values used for IKE are generated using a FIPS-approved X9.31-based pseudo random number generator (PRNG);
- Certificate-based IKE requires external CA-issued X.509v3 certificates. Validity of the certificate path is verified. Certificate revocation checking is supported over the HTTP , LDAP or OCSP protocols;
- IPSec ESP is used to tunnel packets to and from the peer:
  - Packets are encrypted using Triple DES with Keying Option 1, or AES in CBC mode;
  - HMAC-SHA-1 is used for validating packet integrity;
- IKE and IPSec are implemented using a FIPS 140-2 conformant cryptographic module.

6.1.3.2. SSL VPN

The SSL VPN capability is implemented using a combination of a remote access VPN client (SSL Network Extender or SecureClient Mobile client) and the Check Point VPN-1 Power/UTM appliance. The TOE allows users to download the SSL Network Extender client as a lightweight signed ActiveX control or signed Java applet that is automatically

installed on their workstation. Users can also download both clients from the TOE as installable images and install them manually.

The client establishes a lightweight service (daemon) and a virtual network adapter on the workstation. The client uses cryptographic services provided by the workstation environment to establish a TLSv1.0-based secure channel with a TOE appliance. The TOE assigns an IP address to the virtual network adapter and all SSL VPN traffic to and from the workstation is routed through this adapter, protected by the secure channel.

TOE appliances handle SSL VPN traffic as follows:

- The appliance accepts the establishment of a cryptographic tunnel initiated by the client, using the TLSv1.0 protocol:
  - Authentication is performed via RSA signatures, or via single-use passwords that are authenticated with the support of an authentication server in the IT environment;
  - PKCS#1 encoding is used for RSA. Key sizes of 1024, 2048 and 4096 bits are supported;
  - SHA-1 is used as the integrity algorithm;
  - All random values used for TLS are generated using a FIPS-approved X9.31-based pseudo random number generator (PRNG);
  - Packets are encrypted using Triple DES with Keying Option 1;
- Certificate-based authentication requires external CA-issued X.509v3 certificates. Validity of the certificate path is verified. Certificate revocation checking is supported over the HTTP, LDAP, or OCSP protocols;
- TLS is implemented using a FIPS 140-2 conformant cryptographic module.

6.1.3.3. SFR Mapping

The following SFRs are satisfied by the VPN SF:

- **FCS_CKM.2(1)**, **FCS_COP.1(1)**, **FCS_COP.1(2)**, **FCS_COP.1(3)**, **FCS_COP.1(4)**, **FCS_COP.1(5)**, **FCS_COP.1(6)** and **FCS_COP.1(7)** – these requirements are met by the IPSec VPN and SSL VPN capabilities, as follows:
  - FCS_CKM.2(1), FCS_COP.1(5), FCS_COP.1(6), and FCS_COP.1(7) correspond to SA establishment using the IKE protocol.
  - FCS_COP.1(3), FCS_COP.1(4), FCS_COP.1(5) , and FCS_COP.1(6) correspond to cryptographic support for the IPSec protocol.
  - FCS_COP.1(2), FCS_COP.1(5), and FCS_COP.1(6) correspond to cryptographic support for the TLS protocol used for the SSL VPN capability.
  - FCS_COP.1(1) refers to the use of IPSec for encryption of remote administrator session, as described in section 2.3.7. Evaluated configuration guidance instructs the administrator to configure the IPSec VPN SF capa-

bility for protection of traffic between a remote administrator Management GUI and the SmartCenter Server (see Figure 2-4).

- **FCS_CKM.2(2)** – the SSL VPN capability distributes cryptographic keys for SSL VPNs in accordance with the TLSv1.0 protocol.
- **FDP_IFF.1(3)** – the VPN SF performs the valid decryption of incoming traffic and the encryption of outgoing traffic.
- **FDP_UCT.1** and **FDP_UIT.1** – Both IKE/IPSec and the TLS protocols provide transmitted and received objects with protection from unauthorized disclosure. They also protect the data from modification, deletion, insertion and replay conditions, detecting such errors on receipt of data. Refer to [RFC2401] and [RFC2246] for discussions of these properties for the IKE/IPSec and TLS protocols, respectively.
- **FTP_ITC.1** – The IPSec VPN capability provides a communication channel that provides assured identification of its end points using the IKE protocol, protection of the channel data from modification or disclosure using IPSec. Either the TOE or its IPSec VPN peer can initiate the IPSec Security Association. The SSL VPN capability provides a communication channel that provides both assured identification of its end points and protection of the channel data from modification or disclosure using TLS. The TLS session with the TOE is initiated by the remote access VPN client.

6.1.4. Audit

6.1.4.1. Traffic-related Audit Generation

The Stateful Inspection SF supports selective audit record generation for every matched event.

The following security-relevant information is included within each audit record associated with the enforcement of a Packet Inspection policy rule:

- date and time of the event;
- network interface;
- direction (inbound/outbound) of packet flow;
- presumed source and destination IP addresses;
- identification of applicable policy rule;
- transport layer protocol;
- service;
- action (accept, reject, drop) taken; and
- encryption, authentication, and user identification information (if applicable).

6.1.4.2. *Security Server Audit Generation*

The Security Servers selectively log the following events:

- Successful and unsuccessful user authentication events; and
- Protocol validation errors.

Audit record attributes are as for the Traffic-related Audit Generation capability.

6.1.4.3. *VPN-related Audit Generation*

The VPN SF supports selective audit record generation of the following security-relevant events:

- VPN key exchange (successful or unsuccessful) including identity of VPN peer;
- Encryption/decryption of network traffic; and
- VPN packet handling errors.

6.1.4.4. *Audit Collection and Recording*

Check Point VPN-1 Power/UTM appliances record audit records in log files. Log files are periodically switched over to new versions, so that the previous file can be closed and sent to the SmartCenter Server. In addition, the audit records are forwarded online to the SmartCenter Server (in batches of every two seconds) for viewing in SmartView Tracker.

When disk space on the SmartCenter Server falls below a predefined threshold the SmartCenter Server stops collecting audit records. If the disk space on the appliance falls below another predefined threshold, the appliance is configured to transition into a fail-safe mode in which it no longer accepts any incoming or outgoing packets. This ensures that no audit records are lost in the event of storage exhaustion.

In the event of failure, e.g. loss of power, some audit records may be lost. Records lost would be any record that was queued for writing to the log file at the time of the failure event. Unless the appliance is operating at close to a 100% CPU usage, this would encompass only a fraction of a second of audit records.

In case of attack, where a large number of events are generating a large number of audit records in a short period of time, an internal kernel log buffer may be overrun, and audit records lost. TOE installation guidance provides instructions on how to set the log buffer to any arbitrary size as a function of the expected operational profile for audit generation, to prevent this occurrence. In addition, an authorized administrator can monitor disk, memory and CPU resources on both Check Point VPN-1 Power/UTM appliances and the SmartCenter Server. Alerts are generated when these resources fall below a defined threshold, prompting the administrator to take action to ensure that adequate resources are available for audit recording.

6.1.4.5. SmartCenter Server Audit

Administrators manage the TOE by accessing the SmartCenter Server. Administrators do not access Check Point VPN-1 Power/UTM appliances directly in the TOE evaluated configuration. Administrator access is audited on the SmartCenter Server.

The SmartCenter Server maintains separate log files for audit records sent from Check Point VPN-1 Power/UTM appliances and for audit records generated by the SmartCenter Server.

The SmartCenter Server will record the following security-relevant events:

- successful and unsuccessful attempts to log on as administrator;
- locking and unlocking of administrator accounts;
- changes to the configuration of the TOE including: security policies, audit log management, user management, modification of administration attributes assigned to an administrator;
- installation of security policies on Check Point VPN-1 Power/UTM appliances; and
- maintenance of audit log e.g. start of new log, switching of audit log.

The following information will be recorded within each SmartCenter Server audit record:

- date and time;
- type of event;
- object (e.g. Firewall, firewall policy) associated with the event;
- identity of the administrator initiating the event;
- success or failure of the event; and
- details of the changes arising from the event.

6.1.4.6. Audit Review

The SmartView Tracker Management GUI displays audit trail records stored on the SmartCenter Server. Audit review is available to both authorized administrators and authorized audit administrators.

Audit records are displayed in human-readable form from the current or a specified audit log file.

Administrators can search for audit records as well as filter the viewed audit records by a number of record attributes, including the following security-relevant attributes:

- date and time;
- action taken by Check Point VPN-1 Power/UTM appliance or success or failure of administrator action;
- requested service;

- source and destination addresses;
- matched security policy rule or type of administrator action; and
- user identification (if available).

Filters are cumulative and can be defined for either single attribute values or ranges of attribute values.

6.1.4.7. Status Monitoring

The SmartView Monitor Management GUI displays Check Point VPN-1 Power/UTM appliance operational status, policy installation status, and CPU, memory and disk resource levels. Thresholds can be set for monitored values that can generate alerts when exceeded.

6.1.4.8. Alerts

Auditable events may be configured by the authorized administrator to generate alerts. When these events occur they will give rise to a real time alert, in addition to being recorded in the audit log. The product allows alerts to be reported as SNMP traps that can be monitored by standard network management tools, or as GUI alerts which will be displayed in a status window of the SmartView Monitor Management GUIs.

6.1.4.9. SFR Mapping

The following SFRs are satisfied by the Audit SF:

- **FAU_GEN.1** – the Traffic-related Audit Generation, Security Server Audit Generation, VPN-related Audit Generation and SmartCenter Server Audit capabilities generate the required audit records, as shown in the following table derived from Table 5-2 - Auditable Events:

Table 6-2- Audit SF Mapping to FAU_GEN.1

Functional Component	Auditable Event	Capability	Mapping
FAU_GEN.1	Start-up and shutdown of audit functions	N/A	Audit functions start-up when an appliance or SmartCenter Server host boots up, and cannot be disabled by the authorized administrator. Host status can be monitored via the *Self Testing* capability of the TSF Protection SF.
FAU_GEN.1	Access to the IDS System	SmartCenter Server Audit	Logging of administrator logins to Management GUIs.

Functional Component	Auditable Event	Capability	Mapping
FAU_GEN.1	Access to the TOE and System Data	SmartCenter Server Audit	Logging of administrator logins to the Management GUIs. Object modifications are also logged, including the object ID and modified values.
FAU_SAA.3	Enabling and disabling of any of the analysis mechanisms	SmartCenter Server Audit	The IDS System analysis mechanisms are enabled and disabled through the installation of a security policy on TOE appliances; these events are logged by SmartCenter Server.
	Automated responses performed by the tool	Traffic-related Audit Generation, Alerts	Accept, reject, drop and alert actions that are taken as a result of a Packet Inspection match are selectively logged.
FAU_SAR.1	Reading of information from the audit records	SmartCenter Server Audit	Logging of administrator logins to the SmartView Tracker Management GUI.
FAU_SAR.2	Unsuccessful attempts to read information from the audit records	SmartCenter Server Audit	Logging of administrator login failures to the SmartView Tracker Management GUI.
FAU_SEL.1	All modifications to the audit configuration that occur while the audit collections functions are operating	SmartCenter Server Audit	Logging of audit configuration modifications.
FAU_STG.3	Actions taken due to exceeding of a threshold	Alerts	Logging of alert sent when a threshold is exceeded.
FAU_STG.4	Actions taken due to the audit storage failure	Alerts	Logging of alert sent when audit storage failure occurs.
FCS_COP.1	Success and failure, and the type of cryptographic operation	VPN-related Audit Generation	Logging of VPN key exchanges, encryption/decryption of network traffic and packet handling errors.
FIA_UAU.1	Any use of the authentication mechanism.	SmartCenter Server Audit Security Server Audit Generation	Logging of successful and unsuccessful administrator logins, Security Server user authenti-cation events and logging of identity of IPSec peer (for IKE
FIA_UAU.5	The final decision on		

Functional Component	Auditable Event	Capability	Mapping
	authentication.	VPN-related Audit Generation	authentication).
FIA_UID.2	All use of the user identification mechanism.	Traffic-related Audit Generation	Logging of matched packets including presumed source IP address.
FIA_USB.1	Success and failure of binding of user security attributes to a subject (e.g. success or failure to create a subject).	Traffic-related Audit Generation Security Server Audit Generation VPN-related Audit Generation SmartCenter Server Audit	Logging of Stateful Inspection events, including both *Packet Inspection* and packets that are dropped by the *Anti-Spoofing* capability. Logging of successful and unsuccessful administrator logins, Security Server user authenti-cation events and logging of identity of IPSec peer (for IKE authentication).
FDP_IFF.1	All decisions on requests for information flow.	Traffic-related Audit Generation	Logging of Packet Inspection events.
FDP_UCT.1	All VPN security association establishments.	VPN-related Audit Generation	Logging of VPN key exchange events.
FDP_UIT.1	All VPN security association establishments.	VPN-related Audit Generation	Logging of VPN key exchange events.
FMT_MOF.1	Use of the functions listed in this requirement pertaining to audit.	SmartCenter Server Audit	Logging of audit log management.
	All modifications in the behavior of the functions of the TSF	SmartCenter Server Audit	Logging of security policy modifications, SIC registrations.
FMT_MSA.3	Modifications of the default setting of permissive or restrictive rules.	SmartCenter Server Audit	Logging of security policy modifications.
	All modifications of the	SmartCenter	Logging of security policy

Functional Component	Auditable Event	Capability	Mapping
	initial value of security attributes.	Server Audit	modifications.
FMT_MTD.1	All modifications to the values of TSF data	SmartCenter Server Audit	Logging of security policy modifications, user management.
FMT_SMF.1	Use of the management functions.	SmartCenter Server Audit	Logging of administrator logins to the Management GUIs.
FMT_SMR.1	Modifications to the group of users that are part of the authorized administrator role.	SmartCenter Server Audit	Logging of user management operations.
	Unsuccessful attempts to authenticate the authorized administrator role.	SmartCenter Server Audit	Logging of unsuccessful attempts to log on as administrator.
FPT_AMT.1	Execution of the tests of the underlying machine.	Status Monitoring	Monitoring of CPU, memory and disk resource levels.
FPT_TST.1	Execution of the TSF self tests and the results of the tests.	Status Monitoring	Monitoring of operational status and of policy installation status.
FPT_STM.1	Changes to the time.	Traffic-related Audit Generation	Logging of NTP responses.
FTP_ITC.1	All attempted uses of the trusted channel functions.	VPN-related Audit Generation	Logging of VPN key exchange events and encryption/decryption of network traffic.
FTP_TRP.1	All attempted uses of the trusted path functions	SmartCenter Server Audit	Logging of administrator logins to the Management GUIs.

- **FAU_GEN.2** – the Traffic-related Audit Generation, Security Server Audit Generation, VPN-related Audit Generation and SmartCenter Server Audit all re-cord the identity of the user (as defined for FIA_UID.2) that caused the event.
- **IDS_ANL(EXP).1** - the Traffic-related Audit Generation capability records within each analytical result (manifested as a match against an INSPECT rule) the following information required by IDS_ANL(EXP).1: date and time of the result,

type of result (rule number matched), and identification of data source (source IP address).

- **IDS_SDC(EXP).1** - the Traffic-related Audit Generation capability collects the following information from network traffic flowing through the TOE: service requests (access to network services), network traffic, and detected known vulnerabilities (matched INSPECT rules). For each event, the audit record contains the following information required by IDS_SDC(EXP).1: date and time of the event, type of event (rule number matched), subject identity (presumed source IP address), the outcome of the event (accept, drop, or reject), and in addition: protocol, service, and destination address.

  For detected known vulnerabilities, the identification of the know vulnerability is the name of the rule matched by the traffic.

- **FAU_SAR.1**, **FAU_SAR.2**, **FMT_MTD.1(3)** and **IDS_RDR(EXP).1** – these SFRs are met by the Audit Review capability, which allows only authorized administrators and authorized audit administrators access to the SmartCenter Server in order to review audit logs, and lets these administrators review the logs in human readable form.

- **FAU_SAR.3** – The ability to perform searches and sorting of audit data is met by the Audit Review capability.

  The requirement for *sorting* is interpreted as in [I-0388], i.e. grouping items into kinds or classes, and separating information in a particular class from other data, rather than *ordering* which involves arranging the items in a particular sequence. The Audit Review capability meets the sorting requirement by providing a filtering capability.

  Searched and sorted attributes include the following required attributes: user identity; presumed subject address (source address); ranges of dates and times; ranges of addresses; type of event (matched security policy rule); and success or failure of related event (action taken).

- **FAU_SEL.1** – the Traffic-related Audit Generation, Security Server Audit Generation and VPN-related Audit Generation capabilities allow the authorized administrator to configure what events generate audit records.

- **FAU_STG.2** and **IDS_STG(EXP).1** – audit records are protected from unauthorized deletion and unauthorized modifications. The Audit Collection and Recording capability ensures that all stored audit records are maintained in case of audit storage exhaustion, failure and/or attack, and that only a very small number of records that have not yet been stored might be lost in case of failure or attack.

- **FAU_STG.3** - the Audit Collection and Recording capability generates Alerts when disk capacity falls below a defined threshold.

- **FAU_STG.4** and **IDS_STG(EXP).2** – the Audit Collection and Recording capability prevents auditable events when the audit trail is full. Alerts are sent

when the TOE enters fail-safe mode as a result of disk space exhaustion. No audit records are lost when the audit trail is full.

- **IDS_RCT(EXP).1** – the Alerts capability meets the requirement to send an alarm when an intrusion is detected.

6.1.5. Security Management

6.1.5.1. Management Functions

The SmartView Tracker Management GUI provides the authorized administrator and the authorized audit administrator with the capability to perform audit queries as described for the Audit SF in section 6.1.4.6.

The SmartView Monitor Management GUI provides the authorized administrator with the capability to set thresholds for monitored values, as described for the Audit SF Status Monitoring capability in section 6.1.4.7.

All other management functions listed in Table 5-3 are provided to the authorized administrator via the SmartDashboard Management GUI. Table 6-3 describes for each of these management functions the corresponding management functionality provided by the Management GUI.

Table 6-3- Management GUI Management Functions

Component	Management Function	Management Functionality
FMT_MOF.1 (1)	Startup and shutdown of the TOE	TOE start up and shutdown are restricted in the TOE evaluated configuration because there is no administrator interface that allows the authorized administrator to perform these actions. Enabling and disabling the operation of a Check Point VPN-1 Power/UTM appliance can be performed by installing an appropriate policy; for example, the administrator can install a policy that denies all incoming or outgoing traffic apart from management traffic.
	Management of multiple authentication mechanisms	SIC certificates for administrators are managed by the authorized administrator. Authentication of VPN peers is configured by the authorized administrator, including trusted CAs and certificate revocation distribution points. Shared secret authentication can also be configured by the authorized administrator role. IKE authentication of peer external IT entities is

Component	Management Function	Management Functionality
		configured through definition of appropriate VPN communities by the authorized administrator. Shared secrets used for NTP authenticators are set up during installation and generation of the TOE and cannot be modified by the authorized administrator in the TOE evaluated configuration. Shared secrets used for RADIUS server authentication can be configured by the authorized administrator in the RADIUS server objects in the Objects Database. An authorized administrator can configure RADIUS and SecurID server objects in the Objects Database and require single-use password authentication for specific users or user groups.
FMT_MOF.1 (2)	Audit trail management	An authorized administrator can configure the audit log file behavior for a Check Point VPN-1 Power/UTM appliance using the SmartDashboard Management GUI. The administrator determines when and how audit records are forwarded to the SmartCenter Server. The SmartView Tracker Management GUI allows the authorized administrator to perform log switches (changing the output log file), pull log files from Check Point VPN-1 Power/UTM appliances that do not forward their logs automatically, and to purge all records in the active log file.
	Backup and restore for TSF data, information flow rules, and audit trail data	Backup and restoration operations for TSF data, information flow rules, and audit trail data to detachable media are restricted when the TOE is operational. Backup can be scheduled during installation and generation of the TOE, and restoration can be performed from a previously performed backup during installation and generation of the TOE. The SmartDashboard and SmartView Tracker Management GUIs allow the authorized administrator to create backup copies of TSF data,

Component	Management Function	Management Functionality
		information flow rules, and audit trail data on the SmartCenter Server machine, and to revert to a previous revision from these files.
	Control of communication with authorized external IT entities	External IT entities that communicate with the TOE must be defined as objects using the SmartDashboard Management GUI, and appropriate information flow rules configured to allow this communication.
FMT_MOF.1 (3)	Modifying IDS System behaviour	The authorized administrator can load SmartDefense Updates through the SmartDashboard Management GUI.
FMT_MOF.1 (4)	Enabling or disabling ICMP and Check Point RDP support	Support for ICMP and Check Point RDP is enabled and disabled by configuring appropriate information flow rules in the SmartDashboard Management GUI.
FMT_MOF.1 (5)	Enabling SIC connectivity between management and appliance	Enabling SIC connectivity between the SmartCenter Server and an appliance is performed during installation and generation of the appliance, in conjunction with corresponding definitions entered in the SmartDashboard Management GUI.
FMT_MSA.1 (1), FMT_MSA.1 (3)	Management of unauthenticated information flow control rules	Information flow control rules are configured through the SmartDashboard Management GUI, which controls the compilation and installation of the rules as a security policy on TOE appliances.
FMT_MSA.1 (2), FMT_MSA.1 (4)	Management of authenticated information flow control rules	Authenticated rules are configured in the same way as unauthenticated rules; in addition, the authorized administrator requires authentication to be performed for these services.
FMT_MSA.1 (5)	Management of VPN rules	VPN communities and configuration are controlled by the authorized administrator using the SmartDashboard Management GUI.
FMT_MSA.3	Specification of alternative initial values to override the restrictive default values for information flow security	The authorized administrator can enable/disable the implied rules through the SmartDashboard Management GUI, as well as override them with alternative rules.

Component	Management Function	Management Functionality
	attributes	
FMT_MTD.1 (1)	Management of user security attributes	User security attributes can be managed through the SmartDashboard Management GUI.
FMT_MTD.1 (3)	Management of TOE data and performing audit queries	The SmartDashboard Management GUI allows the authorized administrator to manage TOE data. Audit queries are performed via the SmartView Tracker Management GUI.
FMT_MTD.1 (4)	Management of the thresholds and actions taken in case of imminent audit storage failure	The SmartDashboard Management GUI and the SmartView Monitor Management GUI both allow the authorized administrator to define thresholds for required free disk space and to enable the generation of an Alert when the threshold is exceeded.

6.1.5.2. Administrator Access Control

The SmartCenter Server maintains a user database. The user database is distributed to TOE Check Point VPN-1 Power/UTM appliances. The user database contains entries for both administrators and other users of the TOE.

For each user, the user database stores the following security-relevant attributes:

- User identification;
- Association with an administrator permissions profile;
- Single-use password authentication method, IKE shared-secret or certificate (administrators use only certificate-based authentication in the TOE evaluated configuration); and
- Group memberships (if any).

When creating an administrator entry in the user database, the user must be associated with a permission profile. There are four high-level permission classes:

- None – restricts the user from accessing any of the Management GUIs
- Read/Write All – Allows full access (Read/Write) to all three Management GUIs. An additional modifier, Manage Administrators, is required for an administrator to be able to manage administrator user attributes.
- Read Only All – Allows the administrator to access all three Management GUIs with all permissions set to Read Only, restricting him or her from performing any modifications to the TOE or to TOE data.

- Customized – provides more granular control over administrator restrictions. The Manage Administrators permission is only available for Read/Write All.

The SmartCenter Server restricts all management functions according to the user's permission profile, as detailed in Table 6-4 below. For each management function, the required permission is noted in column 2, with column 3 specifying a required modifier (e.g. Read/Write) if any. A user that has not been allocated an appropriate permission will be prevented from performing the corresponding function specified in column 1.

Table 6-4 - Security-relevantAdministrator Permissions

Management function	Permission	Required Modifier
Management of administrator user security attributes	Manage Administrators	
Management of TOE data (network, services, servers, etc.)	Objects Database	Read/Write needed for database modification
Management of non-administrator user security attributes	Check Point Users Database	Read/Write needed for database modification
Modification and installation of the rule base on Check Point VPN-1 Power/UTM appliances	Security Policy	Read/Write needed for policy modification and installation
Access to SmartView Monitor	Monitoring	
Access to SmartView Tracker and Check Point VPN-1 Power/UTM appliance audit records	Track Logs	Read/Write needed for audit trail management
Access to SmartView Tracker and SmartCenter Server audit records	Audit Logs	Read/Write needed for audit trail management

6.1.5.3. SFR Mapping

The following SFRs are satisfied by the Security Management SF:

- **FIA_ATD.1** – the Administrator Access Control capability maintains a database of users, including identity, authorizations information, association with group memberships, and authentication data.
- **FMT_SMR.1** – The authorized administrator role corresponds to the Read/Write All with Manage Administrators permission class. The authorized administrator role may perform all management functions.

  The authorized audit administrator role corresponds to a Custom permission profile with Objects Database, Check Point Users Database, Monitoring, Track Logs and Audit Logs permissions in Read Only mode, respectively. This permission profile restricts the authorized audit administrator to viewing audit records and to monitoring TOE resource values. In particular, an authorized audit administrator is prevented from logging in to the SmartDashboard Management GUI.

A human user may be associated with these roles as described for the Administrator Access Control capability. Permission profiles that contain a subset of the permissions of the authorized administrator role but are not the authorized audit administrator role may also be defined. For the purpose of this ST, they are considered to be authorized administrators.

- **FMT_MOF.1(1)** – Policy installation is restricted to users that have been given the Security Policy permission, i.e. to the authorized administrator role.

  Enabling or disabling multiple use authentications as described in FIA_UAU.5 is restricted to the authorized administrator role via the Manage Administrators, Objects Database, Check Point users database and Security Policy permissions.

- **FMT_MOF.1(2)** - audit trail management is restricted to users with the Objects Database, Track Logs and Audit Logs permissions in Read/Write mode. Backup and restoration for TSF data, information flow rules, and audit trail data require Read/Write permissions. Management of the communication of authorized external IT entities with the TOE is restricted to users with the Objects Database and Security Policy permissions. All of these permissions are available only to the authorized administrator role.

- **FMT_MOF.1(3)** – the behavior of the functions of IDS System data collection, analysis and reaction is controlled through installation of appropriate security policies on Check Point VPN-1 Power/UTM appliances. This is restricted to users with the Security Policy permission, i.e. to the authorized administrator role.

- **FMT_MOF.1(4)** - enabling and disabling ICMP and Check Point RDP are restricted to users with the Security Policy permission, i.e. to the authorized administrator role.

- **FMT_MOF.1(5)** – enabling SIC is restricted to users with the Objects Database permission, i.e. to the authorized administrator role.

- **FMT_MSA.1(1), FMT_MSA.1(3)** - the ability to delete, modify or add Stateful Inspection rules is restricted to a user with the Security Policy permission, i.e. to the authorized administrator role.

- **FMT_MSA.1(2), FMT_MSA.1(4)** – the ability to delete, modify or add Security Server rules is restricted to a user with the Security Policy permission, i.e. to the authorized administrator role.

- **FMT_MSA.1(5)** - the ability to create, query, modify or delete VPN rules is restricted to a user with the Security Policy permission, i.e. to the authorized administrator role.

- **FMT_MTD.1(1)** - the ability to query, modify, delete, and assign user attributes is restricted to a user with the Manage administrators or Check Point Users Database permissions for administrators and other users, respectively, i.e. to the authorized administrator role.

- **FMT_MTD.1(2)** – the Security Management SF does not provide any administrator interface that supports the modification of the time and date.

- **FMT_MTD.1(3)** – the authorized administrator may query and modify all TOE data. An authorized audit administrator has Read Only access to the SmartView Tracker interface, and may only query IDS System and audit data.
- **FMT_MTD.1(4)** – management of thresholds and actions taken in case of imminent audit storage failure is performed through SmartDashboard, restricted to the authorized administrator role.
- **FMT_SMF.1** - the Management Functions capability meets this requirement directly.

6.1.6. SIC

6.1.6.1. Internal CA (ICA)

An internal CA generates X.509v3 certificates that are used for internal communications between the parts of the TOE: the SmartCenter Server, the Check Point VPN-1 Power/UTM appliances, and Management GUI hosts.

Certificates can be issued for PKCS#1 encoded RSA keys of lengths 1024, 2048 or 4096 bits. Certificates represent the SmartCenter Server, the Check Point VPN-1 Power/UTM appliances, and human administrators.

The internal CA publishes CRLs internally to the different parts of the TOE.

6.1.6.2. Secure Internal Communications

Management protocols between the parts of the TOE: the SmartCenter Server, Check Point VPN-1 Power/UTM appliances, and Management GUI hosts are protected using the TLSv1.0 protocol ([RFC2246]).

An ICA-issued certificate is used to authenticate the administrator.

Triple DES (with 192 bit keys as defined in [FIPS PUB 46-3]) is used for encrypting SIC communications.

6.1.6.3. SFR Mapping

The following SFRs are satisfied by the SIC SF:

- **FCS_CKM.2(2)** – SIC distributes cryptographic keys using TLSv1.0.
- **FCS_COP.1(2)** , **FCS_COP.1(5)**, **FCS_COP.1(6)** – SIC uses the following cryptographic algorithms: RSA for authentication, SHA-1 for message digest, and Triple DES for encryption.
- **FPT_ITT.1** – SIC protects management protocols between the separate parts of the TOE from disclosure and modification.
- **FTP_TRP.1** – administration of the TOE is performed over SIC channels between the Management GUI and the SmartCenter Server, providing assured

identification of the two end points and protection of the communicated data from modification or disclosure.

6.1.7. Identification and Authentication (I&A)

6.1.7.1. Single-Use Password Authentication

The TOE in its evaluated configuration supports the use of authentication servers in the IT environment for user authentication via single-use passwords. The RADIUS and SecurID protocols are supported for this purpose.

Note: TOE guidance requires that the authentication server must be installed in a network segment that is protected from any untrusted users by a TOE appliance. If other parts of the TOE interact with the authentication server (i.e. other TOE appliances or the SmartCenter Server), the part of the communication path that is within the TOE must be protected from modification.

6.1.7.2. Administrator Authentication

Administrators authenticate via the Management GUI to the SmartCenter Server. Prior to authentication, the SmartCenter Server does not allow any interaction with the administrator. A trusted path is established between the Management GUI and the SmartCenter Server (using the SIC SF). Authentication is performed via SIC certificates.

6.1.7.3. User Authentication

Users sending or receiving information through the TOE can be authenticated by either setting up a VPN rule that requires a remote access VPN tunnel to be used by the user for sending information through the TOE (via the VPN SF), or configuring a Security Server to require single-use password authentication using an authentication server in the IT environment (via the Security Server SF).

In the evaluated configuration, administrator guidance instructs the administrator to require a single-use authentication mechanism (implemented using IKE, RADIUS or SecurID) for Telnet and FTP (if these services are allowed).

6.1.7.4. External IT Entity Authentication

The external IT entities identified in this ST that must access the TOE (this statement excludes external IT entities that are accessed **by** the TOE, such as CVP and UFP servers) are peer VPN gateways and hosts, NTP servers that are authorized to synchronize the TOE's time and date, and RADIUS authentication servers that may return authentication verdicts for single-use password authentication queries.

Peer IPSec VPN gateways and hosts authenticate to the TOE using IKE (via the VPN SF). NTP and RADIUS servers authenticate via single-use authenticators defined in the NTP and RADIUS protocols, respectively.

6.1.7.5. User Identification

Administrators identify themselves to a Management GUI before they are allowed any other action.

All users sending information through the TOE, whether authenticated or not, will always be identified at least by a source network identifier (IPv4 address).

Authenticated users are further identified in the process of authentication: for authentication via a remote access VPN, user identification is transferred as part of the IKE or TLS protocols; for single-use password authentication, identification is via an entered user name.

The user identity is associated with subjects acting on behalf of the user. It is recorded in all applicable auditable events, and is used to enforce information flow control policies, either directly, or through association with user groups defined by the authorized administrator.

Where the user's network identifier is modified by the TOE (NAT), the original identifier is used for audit and information flow control.

6.1.7.6. SFR Mapping

The following SFRs are satisfied by the I&A SF:

- **FIA_UAU.1** – all users, human and otherwise, must authenticate to the TOE before they are allowed to perform any action except for requesting unauthenticated connectivity queries from the TOE and sending unauthenticated information through the TOE.
- **FIA_UAU.5** – the I&A SF meets this requirements as follows:
  - Administrators authenticate using a SIC certificate-based authentication mechanism.

    When a SIC certificate is used for authenticating the administrator, the administrator enters a multiple-use password that unlocks the use of his private key credential, stored in either a PKCS#12 file. The private key is then used to provide client authentication for the SIC key exchange. In the course of the SIC session establishment, random (single-use) secrets are exchanged between the session peers. The TLS protocol is resistant to replay attacks. Thus SIC certificate-based authentication can be considered to be a single-use mechanism, with similar justification to the justification used in [PD-0105] for IKE.
  - External IT entities accessing the TOE authenticate using IKE, or using NTP or RADIUS protocol single-use authenticators. [PD-0105] provides guidance that IKE is an acceptable single-use authentication mechanism for the firewall PPs.
  - Human users sending information through the TOE are authenticated via the User Authentication capability.

- **FIA_UID.2** – All users are identified before any other TSF-mediated actions are allowed on behalf of the user.
- **FIA_USB.1** - this requirement is met directly by the User Identification capability, which associates the user identity with subjects acting on behalf of the user. The user identity is recorded in all applicable audit records, and is used to enforce information flow control policies, either directly, or through association with user groups defined by the authorized administrator.

6.1.8. TSF Protection

6.1.8.1. Domain Separation

The principal TSF functionality, including information flow control, IDS/IPS and VPN, are implemented on a self-contained hardware appliance running a stripped-down version of the Linux operating system. The appliance does not contain untrusted processes or users. It does not depend on any component in the IT environment for its protection from interference and tampering by untrusted users.

The management components of the TOE are all protected from interference and tampering by untrusted users by a Check Point VPN-1 Power/UTM appliance, that prevents any external access to these components.

The security domains of controlled subjects are separated by the virtue of the use of separate network interfaces or VLANs, such that all traffic between TOE interfaces is mediated by the TSF.

6.1.8.2. Virtual Defragmentation

When IPv4 packets that are fragmented are received by the Check Point VPN-1 Power/UTM appliance, they are first reassembled before being inspected. Only well-formed packets are passed on to packet inspection.

6.1.8.3. Boot Security

During the Check Point VPN-1 Power/UTM appliance boot process, there is a lag between the time when the network interface is operational, and the time that the Stateful Inspection functionality is fully functioning. During this time, Boot Security is enforced:

- Traffic flow through the appliance is disabled; and
- Traffic to and from the appliance is controlled by a Default Filter that drops all external traffic to the appliance.

6.1.8.4. Reference Mediation

All network traffic arriving at a TOE network interface is mediated by the TSF once the Check Point VPN-1 Power/UTM appliance is in an operational state.

6.1.8.5. Hardware Clock

The timestamps used for stamping audit records are provided by the underlying operating system that is part of the TOE on both Check Point VPN-1 Power/UTM appliances and the SmartCenter Server. The operating system uses a hardware clock to maintain reliable time even after periods of time when the appliance or server is powered down.

6.1.8.6. Self Testing

When the Check Point VPN-1 Power/UTM appliance is started, it performs a BIOS-level test of the underlying abstract machine. The software then performs FIPS 140-2 cryptographic module tests before it allows any traffic to be mediated by the TOE.

During normal operation, a watchdog process verifies the existence of critical processes. CPU, memory and disk resources are monitored continuously and can be displayed using the SmartView Monitor Management GUI. Thresholds can be set for monitored values that can generate alerts when exceeded.

Policy files are verified when they are received from the SmartCenter Server. Software integrity is verified during startup. Administrators can determine that managed appliances are in operational status via the SmartView Monitor Management GUI.

6.1.8.7. SFR Mapping

The following SFRs are satisfied by the TSF Protection SF:

- **FPT_AMT.1** and **FPT_TST.1** – the Self Testing capability provides both testing of abstract machine resources including memory, disk, and CPU, as well as testing of the correct operation of the cryptographic module, critical processes, and the integrity of software and policy files.
- **FPT_RVM.1** – when the Check Point VPN-1 Power/UTM appliance is powered down, no traffic can traverse its network interfaces. After power-up, the Boot Security capability ensures non-bypassability until the TOE software is operational, at which time the Reference Mediation capability ensures that all traffic is mediated. Virtual Defragmentation ensures that an attacker cannot bypass the TSP by fragmenting IP packets so that packet headers, used for Stateful Inspection, are not available for some of the fragments.
- **FPT_SEP.1** – the reference mediation and domain separation capabilities meet these requirements directly.
- **FPT_STM.1** – the Hardware Clock provides reliable time stamps for the TSF. Audit and IDS System records are stamped with both date and time by the TOE component on which they are generated, and are forwarded to the SmartCenter Server; they are stored in log files and displayed in the order in which they are received, with an indication of the originating component and the local time stamp. In this way, the order of the occurrence of auditable events is preserved.

6.2. TOE Security Assurance Measures

This section describes the assurance measures provided for the TOE, and maps them to the security assurance requirements (SARs) in section 5.2.

The SARs in the ST are exclusively based on CC EALs and other [CC] Part 3 assurance components (namely ALC_FLR.3). The assurance measures are presented in the form of a reference to the documents that show that the assurance requirements are met. These documents are uniquely identified in the configuration list included in the Configuration Management documentation.

6.2.1. Security Target

The Security Target (this document) identifies the Security Functions (SFs) of the TOE, and traces them to the defined set of security requirements.

The ST states that the TOE does not have any permutational and/or probabilistic mechanisms.

6.2.2. Process Assurance Documentation

6.2.2.1. Lifecycle Model

The Lifecycle Model describes the procedures, tools and techniques used by the developer for the development and maintenance of the TOE. The overall management structure is described, as well as responsibilities of the various departments.

Development tools and procedures being used for each part of the TOE are identified, including any implementation-dependent options of the development tools.

Flaw tracking and remediation procedures and guidance addressed to TOE developers describe the procedures used to accept, track, and act upon reported security flaws and requests for corrections to those flaws, as well as the distribution of reports and corrections to registered users. Guidance addressed to TOE users describes means by which TOE users with a valid Software Subscription license report to the developer any suspected security flaws in the TOE, and receive security flaw reports and corrections.

For each developer site involved in the production of the TOE, the documentation describes the measures taken to ensure that the security of the configuration items of the TOE is maintained until shipped to the user.

6.2.2.2. Delivery and Operation

Delivery and Operation procedures describe the measures taken to ensure that the security of the configuration items of the TOE is maintained when distributing the TOE to a user's site, up to the point that the TOE is in its operational state, and how any modifications or discrepancies in the version received at the user's site are detected.

6.2.2.3. Configuration Management

The Configuration Management (CM) documentation includes a CM plan, an acceptance plan, and a configuration list of all configuration items for the TOE, including: implementation representation; security flaws; and the evaluation evidence required by the assurance components in the ST.

The CM plan describes the automated tools used in the CM system, and the means by which these automated tools control changes to the TOE implementation representation and support the generation of the TOE.

6.2.3. Development Documentation

6.2.3.1. Functional Specification

The Functional Specification identifies all of the TOE's security functions and external interfaces, and provides a full description of all external TOE security function interfaces.

6.2.3.2. Security Policy Model

The Security Policy Model is a document that models a subset of the policies of the TSP in informal language, and demonstrates correspondence between the functional specification and the TSP model.

6.2.3.3. High-level Design

The High-level Design document provides a description of the TOE in terms of major structural units (i.e. subsystems) and relates these units to the functions that they provide. Underlying hardware, firmware, and software are identified, as well as subsystem interfaces.

6.2.3.4. Low-level Design

The Low-level Design document provides a description of the internal workings of the TSF in terms of modules and their interrelationships and dependencies

6.2.3.5. Implementation Representation

An evaluator-selected subset of the implementation representation for the TOE will be provided to the evaluators.

6.2.3.6. Analysis of Correspondence

The Analysis of Correspondence is intended to demonstrate to the evaluator that the various provided representations are an accurate, consistent, and complete instantiation of the functions expressed as functional requirements in the ST. This is achieved through a step-wise refinement and the cumulative results of correspondence determinations

between the adjacent abstractions of representation: TOE Summary Specification to Functional Specification, Functional Specification to High-level Design, and High-level Design to Low-level Design. Each of the design documents contains a section that demonstrates correspondence with the preceding level of abstraction, as well as to the set of SFRs defined in the ST. The Analysis of Correspondence document completes this demonstration by mapping the selected subset of the Implementation Representation to the relevant parts of the Low-level Design.

6.2.4. The TOE

Instances of the TOE are provided for independent testing and vulnerability testing.

6.2.5. Test Plan and Procedures

The Test Documentation document describes the testing of the TOE at the level of its functional specification and high-level design. It also contains an Analysis of Coverage and an Analysis of Depth of Testing.

Test documentation consists of test plans, test procedure descriptions, expected test results and actual test results. Test plans identify the security functions tested and describe the goal of the tests to be performed. Test procedures descriptions identify the tests to be performed and describe the scenarios for testing each security function. The match between actual test results and expected test results demonstrates that each tested security function behaved as specified.

6.2.6. Guidance Documentation

Installation, administration, and user guidance documentation (identified in section 0) are provided to the evaluators for evaluation of guidance.

6.2.7. Analysis of Guidance Documentation

The Analysis of Guidance Documentation justifies that the guidance is clear and complete, supporting the TOE administrators in the secure administration of the TOE.

6.2.8. Vulnerability Analysis

The Vulnerability Analysis builds on the other evaluation evidence to show that the developer has systematically searched for vulnerabilities in the TOE and provides reasoning about why they cannot be exploited in the intended environment for the TOE. The analysis references public sources of vulnerability information to justify that the TOE is resistant to obvious penetration attacks.

The Vulnerability Analysis also identifies all permutational or probabilistic security mechanisms and demonstrates that all of the relevant mechanisms fulfill the minimum strength of function claim, 'SOF-medium'.

6.2.9. SAR Mapping

Table 6-5 maps evaluation evidence to SARs, showing that all of the assurance requirements of the TOE are met by appropriate assurance measures.

Table 6-5- Mapping of Evaluation Evidence to Assurance Requirements

Document	ACM_AUT.1	ACM_CAP.4	ACM_SCP.2	ADO_DEL.2	ADO_IGS.1	ADV_FSP.2	ADV_HLD.2	ADV_IMP.1	ADV_LLD.1	ADV_RCR.1	ADV_SPM.1	AGD_ADM.1	AGD_USR.1	ALC_DVS.1	ALC_LCD.1	ALC_TAT.1	ATE_COV.2	ATE_DPT.1	ATE_FUN.1	ATE_IND.2	AVA_MSU.2	AVA_SOF.1	AVA_VLA.2	ALC_FLR.3
Analysis of Correspondence										✓														
Analysis of Guidance Documentation																					✓			
Configuration Management	✓	✓	✓																					
Delivery and Operation				✓	✓																			
Functional Specification						✓				✓														
Guidance Documentation					✓							✓	✓								✓			
High-level Design							✓			✓														
Implementation Representation Subset								✓		✓														
Lifecycle Model														✓	✓	✓								✓
Low-level Design									✓	✓														
Security Policy Model											✓													
Security Target (this document)																								
Test Documentation																	✓	✓	✓					
The TOE																				✓				
Vulnerability Assessment																						✓	✓	

6.3. Identification of Standards

The subject of criteria for the assessment of the inherent qualities of cryptographic algorithms is not covered in the CC. The SFRs in the Cryptographic Support (FCS) class stated in Section 5.1.2 therefore reference external standards that the implementation must meet when providing the required capabilities.

Table 6-6 summarizes the standards compliance claims made in Section 5.1.2 and states for each the method used to determine compliance (aside from development assurances). The method may be an applicable NIST certificate number, other third-party certification, or a vendor assertion.

Note: Check Point VPN-1 Power/UTM cryptographic algorithm certificates are referenced in [FIPSPOL].

Table 6-6- Cryptographic Standards and Method of Determining Compliance

Standard claimed	Cryptographic SFRs	Method of determining compliance
RFC 2409 (IKE)	FCS_CKM.2(1)	Third party testing: ICSA Certification Report dated 9/19/2008
RFC 2406 (ESP)	FCS_COP.1(3)	
FIPS 140-2 Level 1	FCS_CKM.2(1), FCS_COP.1(1), FCS_COP.1(3), FCS_COP.1(4), FCS_COP.1(5), FCS_COP.1(7)	Vendor assertion[46]
X9.31-based PRNG	FCS_CKM.2(1)	Cert. #90
Triple DES in CBC modes as per FIPS PUB 46-3	FCS_COP.1(1), FCS_COP.1(2), FCS_COP.1(3)	Cert. #733
AES in CBC mode as per FIPS PUB 197	FCS_COP.1(3)	Cert. #257
HMAC-SHA-1 as per RFC 2104, FIPS PUB 198 and RFC 2404	FCS_CKM.2(1), FCS_COP.1(4)	Cert. #502
SHA-1 as per NIST PUB FIPS 180-2	FCS_CKM.2(1), FCS_COP.1(5)	Cert. #890
RSA as per PKCS#1	FCS_CKM.2(1), FCS_COP.1(6)	Cert. #66 and #132
TLSv1.0 as per RFC 2246	FCS_CKM.2.1(2)	Vendor assertion

[46] A previous version of the product, NGX (R60), was validated to conform with FIPS 140-2 level 1 (see Cert.#722).

7. PP Claims

7.1. PP Reference

The TOE meets and exceeds all security objectives and requirements of all three PPs listed in section 1.3.3: the two firewall PPs, and the IDS System PP, except for AVA_VLA.3 (in-evaluation at the time of publication of this ST) and the following firewall PP requirements that are inapplicable to the TOE: FIA_AFL.1 and FMT_MTD.2.

7.2. PP Tailoring

This ST was constructed as follows: the security objectives for the TOE include all [APP-PP] and [TFF-PP] security objectives, with the qualifications specified in section 4.1.1. Appropriate [IDSSPP] objectives were then restated, except for objectives identified in section 4.1.2 that were determined to be either substantially equivalent to corresponding firewall PP objectives (with the equivalency identified in section 8.1.1.2), or irrelevant in the context of this ST (see section 8.1.1.2 for exclusion rationale). A similar process was used for deriving security objectives for the environment.

All security requirements from all three PPs have been restated in this ST, except for the SFRs listed above as exceptions. For some requirements, a hierarchical component was selected in place of one or more of the PPs' requirements; by definition a TOE meeting the hierarchical requirement would meet the original requirement as well. Similarly, requirements have been qualified, within the bounds set by the PPs. Permitted operations performed on PP security functional requirements are identified in Table 5-1. In some cases, application notes and footnotes were added in the statement of security functional requirements to clarify the relationship of an SFR to the claimed PPs. Footnotes have also been used to identify requirements that have been tailored to conform to the CCv2.2 syntax.

No operations are applied to assurance components.

7.3. PP Additions

In addition to the security objectives and requirements inherited from the claimed PPs, this ST provides additional objectives and requirements that are intended to serve two purposes:

1. Define VPN functionality for the TOE:
    a. VPN objectives are identified in section 4.1.3;
    b. VPN SFRs are identified in Table 5-1 as 'VPN'; and
2. Support PP or VPN requirements in order to ensure that the requirements in the ST work together to form a mutually supportive and internally consistent whole. These additional requirements are identified in Table 5-1 as 'DEP' or 'Other'.

The assurance level has been augmented in relation to that required in the claimed PPs as described in section 8.2.3.

8. TOE Rationale

8.1. Security Objectives Rationale

8.1.1. IT Security Objectives Rationale

Table 8-1 maps IT security objectives to the defined security environment. The table demonstrates that each threat and OSP is met by at least one security objective, and that each objective meets at least one threat or OSP; this is then followed by explanatory text of how this mapping was derived.

Table 8-1- Tracing of IT security objectives to the TOE security environment

	T.NOAUTH	T.REPEAT	T.REPLAY	T.ASPOOF	T.MEDIAT	T.OLDINF	T.PROCOM	T.AUDACC	T.SELPRO	T.AUDFUL	T.MODEXP	T.TUSAGE	T.MISUSE	T.INADVE	T.MISACT	T.NACCESS	T.NMODIFY	P.CRYPTO
O.IDAUTH	✓											**Countered by non-IT objectives – see below**						
OE.IDAUTH	✓																	
O.SINUSE		✓	✓															
O.MEDIAT				✓	✓	✓												
O.SECSTA	✓								✓									
O.ENCRYP	✓						✓											✓
O.SELPRO	✓								✓	✓								
O.AUDREC								✓										
O.ACCOUN								✓										
O.SECFUN	✓		✓							✓								
O.LIMEXT	✓																	
O.EAL											✓							
O.IDSENS					✓								✓	✓	✓			
O.IDANLZ					✓								✓	✓	✓			
O.RESPON					✓								✓	✓	✓			
O.OFLOWS										✓								
O.INTEGR									✓									
O.VPN																✓	✓	
OE.VPN																✓	✓	

The firewall PP IT security objectives are the core of the security target for the TOE. [IDSSPP] security objectives were added to this ST as appropriate: IT security objectives which were deemed equivalent to corresponding firewall PP objectives are clearly identified in section 4.1.2. Finally, VPN-related security objectives (no PP compliance claimed) were added to the ST. The following subsections describe how these objectives were mapped to security environment considerations.

8.1.1.1. Firewall PP security objectives

The mapping of the Firewall PP IT security objectives (O.IDAUTH through O.EAL) to environmental considerations is identical to the mapping given in [APP-PP], with the exception that O.IDAUTH has been updated to rely on a corresponding objective for the IT environment OE.IDAUTH in order to meet T.NOAUTH (see section 4.1.1).

8.1.1.2. IDS System PP security objectives

The TOE's environment is that of a firewall, and its compliance with the [IDSSPP] is claimed in that context. The TOE's [IDSSPP] security objectives complement the firewall PP objectives by providing finer control over information flow. A firewall strictly enforces a security policy that defines what traffic may or may not flow. An IDS allows an additional level of control by sensing and analyzing network traffic against known attack signatures; traffic that may be indicative of misuse, inadvertent activity and access, and malicious activity is audited, and the TOE may respond more flexibly than a firewall typically can, e.g. may generate an alert rather than deny the information flow.

In addition, some of the [IDSSPP] security objectives are more specific than the firewall PP objectives about the self-protection functionality that must be provided by the TOE.

Table 8-2 lists IT security objectives for the TOE defined in [IDSSPP] that have been omitted from this ST because they are not needed to establish the [IDSSPP] IT security requirements:

Table 8-2 - Omitted [IDSSPP] IT Security Objectives

[IDSSPP] objective	Equivalent in this ST	Omission rationale
O.PROTCT	O.SELPRO	Both O.PROTCT and O.SELPRO require the TOE to protect itself. The two objectives are similar and there is no added benefit gained from restating both.
O.IDSCAN	None – irrelevant as the TOE does not perform scanning; only sensing.	The [IDSSPP] requires that a conformant TOE must include at least one Sensor or Scanner (see [IDSSPP] application note for IDS_SDC.1), but not both. The Check Point VPN-1 Power/UTM IDS provides a Sensor that inspects traffic flowing through the TOE, but does not actively scan protected hosts for vulnerabilities.

[IDSSPP] objective	Equivalent in this ST	Omission rationale
O.EADMIN O.ACCESS	O.SECFUN	Rationale for inclusion of the [IDSSPP] objectives O.EADMIN and O.ACCESS in O.SECFUN is as follows: • Both O.EADMIN and O.SECFUN deal with providing management functionality: O.EADMIN requires the TOE to include a set of functions that allow effective management of its functions and data. O.SECFUN requires the TOE to provide functionality that enables an authorized administrator to use the TOE security functions. • Both O.ACCESS and O.SECFUN deal with restricting management functions: O.ACCESS requires the TOE to allow authorized users to access only appropriate TOE functions and data. O.SECFUN requires the TOE to ensure that only authorized administrators may access such functionality.
O.IDAUTH	O.IDAUTH	The [IDSSPP] O.IDAUTH objective applies to all access to TOE functions and data, whereas the corresponding firewall PP objective, adopted in this ST, allows exceptions (e.g. unauthenticated information flow through the TOE). In addition, the firewall PP allows the allocation of the authentication requirement to the environment, as indicated by OE.IDAUTH. Following is a rationale for why the intention of the [IDSSPP] is not violated. In [IDSSPP], users perform administrative access. In this ST, administrator access to the TOE always requires certificate-based authentication performed exclusively by the TSF. This is in-line with the intention of the [IDSSPP]. Single-use password authentication is performed by the TSF with the assistance of the IT environment, but only when configured by an authorized administrator for users sending information through the TOE.
O.AUDITS	O.AUDREC	O.AUDREC is a generalization of O.AUDITS. O.AUDITS requires the TOE to record audit records for data accesses and use of the System

[IDSSPP] objective	Equivalent in this ST	Omission rationale
		functions. O.AUDREC requires the TOE to provide a means to record a readable audit trail of security-related events; this is a more general statement because data accesses and use of the System functions are security-related.
O.EXPORT	None	Omitted as per the guidance given by [PD-0097].

Where appropriate, [IDSSPP] environment considerations were not copied to this ST. [IDSSPP] IT security objectives were mapped to threats defined in the firewall PPs, showing that these threats are countered by the TOE with the support of the stated [IDSSPP] security objectives, as follows:

T.MEDIAT: *An unauthorized person may send impermissible information through the TOE which results in the exploitation of resources on the internal network.*

In addition to the O.MEDIAT security objective defined in the firewall PPs, the [IDSSPP] objectives O.IDSENS, O.IDANLZ and O.RESPON serve to counter T.MEDIAT by sensing, analyzing, and responding to traffic indicative of misuse.

T.AUDFUL: *An unauthorized person may cause audit records to be lost or prevent future records from being recorded by taking actions to exhaust audit storage capacity, thus masking an attackers actions.*

The [IDSSPP] objective O.OFLOWS requires potential audit and IDS System data storage overflows to be appropriately handled by the TOE.

T.SELPRO: *An unauthorized person may read, modify, or destroy security critical TOE configuration data.*

In addition to the O.SELPRO and O.SECSTA security objectives defined in the firewall PPs to ensure that TOE resources are not compromised during initial start-up of the TOE or recovery from an interruption in TOE service and that the TOE protects itself against attempts by unauthorized users to bypass, deactivate or tamper with TOE security functions, the [IDSSPP] objective O.INTEGR requires the integrity of all audit and IDS System data to be ensured.

The following [IDSSPP] threats were included in this ST because they describe threats that are not necessarily countered by a firewall: activity indicative of misuse, inadvertent activity and access, and malicious activity on an IT System that the TOE monitors. The manifestation of these threats often generates network traffic that is either used for the attack or is symptomatic to it. This traffic can be sensed and analyzed by the IDS System, and appropriate responses taken to counter or mitigate the threat.

T.MISUSE *Unauthorized accesses and activity indicative of misuse may occur on an IT System the TOE monitors.*

The [IDSSPP] objectives O.IDSENS, O.IDANLZ and O.RESPON serve to counter T.MISUSE by sensing, analyzing, and responding to traffic indicative of unauthorized access and activity indicative of misuse on an IT System the TOE monitors.

T.INADVE: *Inadvertent activity and access may occur on an IT System the TOE monitors.*

The [IDSSPP] objectives O.IDSENS, O.IDANLZ and O.RESPON serve to counter T.INADVE by sensing, analyzing, and responding to traffic indicative of inadvertent activity and access on an IT System the TOE monitors.

T. MISACT: *Malicious activity, such as introductions of Trojan horses and viruses, may occur on an IT System the TOE monitors.*

The [IDSSPP] objectives O.IDSENS, O.IDANLZ and O.RESPON serve to counter T.MISACT by sensing, analyzing, and responding to traffic indicative of malicious activity on an IT System the TOE monitors.

[IDSSPP] assumptions are omitted. Assumptions are upheld by objectives for the environment, and their omission cannot weaken the claimed security of the TOE.

[IDSSPP] OSPs are omitted. [IDSSPP] OSPs are not clearly stated, in that they do not refer to corresponding U.S. national or international rules, practices or guidelines. None of the [IDSSPP] IT security objectives is traced solely to an OSP. As explained in [CEMv2.2] paragraph 315, OSPs need not be present in the ST if the security objectives for the TOE and its environment are derived from assumptions and threats only.

8.1.1.3. VPN security objectives

The description of the TOE security environment introduces two additional threats on top of the firewall PP-defined threats, in section 3.2.2, that are countered by the TOE's VPN IT security functionality:

T.NACCESS *An unauthorized person or external IT entity may be able to view data that is transmitted between the TOE and a remote authorized external IT entity.*

T.NMODIFY *An unauthorized person or external IT entity may modify data that is transmitted between the TOE and a remote authorized external IT entity.*

These two threats defined in this ST are countered by O.VPN and OE.VPN, which require the TOE and its VPN peers to protect the confidentiality of data transmitted between the TOE and the peer, and to provide authentication for such data, allowing the receiver of the information to verify that the received data accurately represents the data that was originally transmitted.

8.1.2. Non-IT Security Objectives Rationale

Table 8-3 maps non-IT security objectives to the security environment. The table demonstrates that each assumption is upheld by at least one non-IT security objective for the environment, and that each non-IT security objective upholds at least one assumption or meets at least one threat or OSP; this is then followed by explanatory text of how this mapping was derived.

Table 8-3- Tracing of non-IT security objectives to the TOE security environment

	A.PHYSEC	A.MODEXP	A.GENPUR	A.PUBLIC	A.NOEVIL	A.SINGEN	A.DIRECT	A.NOREMO	A.REMACC	T.NOAUTH	T.AUDACC	T.TUSAGE
NOE.PHYSEC	✓											
NOE.MODEXP		✓										
NOE.GENPUR			✓									
NOE.PUBLIC				✓								
NOE.NOEVIL					✓							
NOE.SINGEN						✓						
NOE.DIRECT							✓					
NOE.NOREMO								✓				
NOE.REMACC									✓			
NOE.GUIDAN											✓	✓
NOE.ADMTRA											✓	✓
NOE.CREDEN										✓		

In addition, this section provides a rationale[47] for why any assumptions stated in this ST that were added above and beyond those stated for any claimed PP do not violate the original intent of the PP. For this purpose, note that all assumptions in this ST are derived from the firewall PPs; therefore, there is no weakening of the security requirements intended by the firewall PPs by an additional [IDSSPP] assumptions. Furthermore, there is a one-to-one correspondence between each firewall PP assumption and a corresponding objective for the non-IT environment. Therefore, this rationale focuses on showing that there is no weakening of the security requirements of any of the claimed PPs caused by the addition of security objectives for the environment.

[47] This rationale was modeled after [PD-0055].

This ST restates the assumptions and the non-IT security objectives for the environment defined in the firewall PPs. [IDSSPP] non-IT security objectives were shown in section 4.2.2 to be equivalent to corresponding firewall PP objectives, except for NOE.CREDEN, which requires access credentials to be protected by the users.

The assumptions and non-IT security and objectives for the environment from the firewall PPs do not serve to weaken the [IDSSPP] security objectives or the original intent of the [IDSSPP] assumptions. This is established as follows:

- NOE.PHYSEC – corresponds to [IDSSPP] O.PHYCAL
- NOE.MODEXP – hosting the IDS System on a medium robustness firewall strengthens rather than weakens the IDS System's self-protection capabilities in relation to that claimed in the [IDSSPP].
- NOE.GENPUR, NOE.PUBLIC – these two security objectives for the environment do not change the IDS System environment in such a way that affects the TOE's meeting of its stated objectives, nor do they change an [IDSSPP] objective from a TOE objective to an environmental objective. They merely add implementation detail that limits the acceptable implementation, and do not violate the original intent of the PP. This is because none of the [IDSSPP] objectives referred to the protection of or from any general purpose computing capabilities and/or public data that might be hosted on the TOE.
- NOE.NOEVIL, NOE.ADMTRA – these two security objectives for the environment correspond to the [IDSSPP] objective for the environment O.PERSON.
- NOE.SINGEN - this security objective for the environment corresponds to the [IDSSPP] objective for the environment O.INTROP, which upholds assumption A.ACCESS that the TOE has access to all the IT System data it needs to perform its functions.
- NOE.DIRECT, NOE.REMACC describe the services that are provided by the TOE to users (direct connection, remote administration) and so are implementation detail that limits the acceptable implementation, and do not violate the original intent of the PP.
- NOE.NOREMO is an objective for the environment that the TOE should not be configured to provide any non-administrative services to remote human users. As no such service is mentioned or referred to in the [IDSSPP], this additional assumption does not violate the original intent of the PP.
- NOE.GUIDAN – this security objective for the environment corresponds to the [IDSSPP] objective for the environment O.INSTAL.

The mapping of the firewall PP non-IT security objectives for the environment to assumptions and threats is identical to that given in the PPs. NOE.CREDEN was mapped to T.NOAUTH, because users must protect their access credentials in order for the TSP to be enforced. This does not serve to weaken the firewall PP TOE security objectives, because user protection of access credentials is consistent with that context as well.

8.2. Security Requirements Rationale

8.2.1. Security Functional Requirements Rationale

Table 8-4 maps claimed SFRs to the defined security objectives for the TOE. The table demonstrates that each security objective is met by one or more SFRs, and that each SFR meets at least one security objective. This is followed by appropriate explanatory text that provides further justification that the mapped SFRs are suitable to meet the security objectives for the TOE.

The mapping of objectives to SFRs is based on the corresponding rationales provided by the firewall and IDS System PPs. In some cases, a mapping defined in [IDSSPP] was omitted here where judged to be redundant. SFRs introduced in this ST are also mapped to corresponding security objectives.

Table 8-4 – TOE Security Objective to Functional Component Mapping

Key: ☑ Mapping taken from firewall PP ◈ Mapping taken from IDS System PP
✓ Mapping added in this ST × Omitted IDS System PP mapping

(Note: where a mapping exists in both firewall and IDS PP, the ☑ symbol is used.)

	O.IDAUTH	O.SINUSE	O.MEDIAT	O.SECSTA	O.ENCRYP	O.SELPRO	O.AUDREC	O.ACCOUN	O.SECFUN	O.LIMEXT	O.EAL	O.IDSENS	O.IDANLZ	O.RESPON	O.OFLOWS	O.INTEGR	O.VPN
FAU_GEN.1							☑	☑	✓		Mapped to Security Assurance Requirements						
FAU_GEN.2								✓									
FAU_SAA.3													✓				
FAU_SAR.1							☑		◈								
FAU_SAR.2	×								◈								
FAU_SAR.3							☑		◈								
FAU_SEL.1							◈		◈								
FAU_STG.2	×			☑		☑			☑						◈	◈	
FAU_STG.3															✓		
FAU_STG.4				☑		☑	◈		☑						◈		
FCS_CKM.2(1)		✓															✓
FCS_CKM.2(2)		✓				✓											✓
FCS_COP.1(1)					☑												
FCS_COP.1(2)						✓											✓

	O.IDAUTH	O.SINUSE	O.MEDIAT	O.SECSTA	O.ENCRYP	O.SELPRO	O.AUDREC	O.ACCOUN	O.SECFUN	O.LIMEXT	O.EAL	O.IDSENS	O.IDANLZ	O.RESPON	O.OFLOWS	O.INTEGR	O.VPN
FCS_COP.1(3)																	✓
FCS_COP.1(4)		✓															✓
FCS_COP.1(5)		✓				✓											✓
FCS_COP.1(6)		✓															✓
FCS_COP.1(7)		✓															✓
FDP_IFC.1(1)			☑														
FDP_IFC.1(2)			☑														
FDP_IFC.1(3)			☑														✓
FDP_IFF.1(1)			☑														
FDP_IFF.1(2)			☑														
FDP_IFF.1(3)			☑														✓
FDP_RIP.2			☑														
FDP_UCT.1																	✓
FDP_UIT.1																	✓
FIA_ATD.1	☑	☑							☑								
FIA_UAU.1	◈								◈								
FIA_UAU.5	☑	☑															
FIA_UID.2	☑							☑	◈								
FIA_USB.1	✓							✓									
FMT_MOF.1(1)				☑					☑	☑							
FMT_MOF.1(2)				☑					☑	☑							
FMT_MOF.1(3)	×					◈			◈								
FMT_MOF.1(4)									✓								
FMT_MOF.1(5)						✓			✓								
FMT_MSA.1(1)			☑	☑					☑								
FMT_MSA.1(2)			☑	☑					☑								
FMT_MSA.1(3)			☑	☑					☑								

	O.IDAUTH	O.SINUSE	O.MEDIAT	O.SECSTA	O.ENCRYP	O.SELPRO	O.AUDREC	O.ACCOUN	O.SECFUN	O.LIMEXT	O.EAL	O.IDSENS	O.IDANLZ	O.RESPON	O.OFLOWS	O.INTEGR	O.VPN
FMT_MSA.1(4)			☑	☑					☑								
FMT_MSA.1(5)									✓								✓
FMT_MSA.3			☑	☑					☑								
FMT_MTD.1(1)									☑								
FMT_MTD.1(2)									☑								
FMT_MTD.1(3)	×					×			⍰							⍰	
FMT_MTD.1(4)									✓								
FMT_SMF.1									✓	✓							
FMT_SMR.1	⍰								☑								
FPT_AMT.1				✓		✓											
FPT_ITT.1						✓											
FPT_RVM.1	×			☑		☑	×		×							×	
FPT_SEP.1	×					☑	×		×							×	
FPT_STM.1							☑										
FPT_TST.1				✓		✓			✓								
FTP_ITC.1	✓																✓
FTP_TRP.1	✓					✓			✓								
IDS_SDC(EXP).1												⍰					
IDS_ANL(EXP).1													⍰				
IDS_RCT(EXP).1														⍰			
IDS_RDR(EXP).1	×								⍰								
IDS_STG(EXP).1	×					⍰			⍰						⍰	⍰	
IDS_STG(EXP).2									✓						⍰		

O.IDAUTH *The TOE with the support of the IT environment must uniquely identify and authenticate the claimed identity of all users, before granting a user access to TOE functions or, for certain specified services, to a connected network.*

FIA_UID.2 ensures that each user is identified before any TSF-mediated actions are allowed, including access to the TOE itself as well as passing traffic through the TOE. FIA_ATD.1 defines the security attributes that are maintained for each user including a unique identity and association with the administrator roles defined in FMT_SMR.1. FIA_USB.1 determines the rules for associating these security attributes with a subject acting on behalf of the user. FIA_UAU.1 mandates that users must be authenticated before they are allowed any TSF-mediated actions except for a defined list of unauthenticated services. FIA_UAU.5 describes the multiple authentication mechanisms that are to be used for authenticating users in different authentication scenarios: remote administrator access to the TOE, authorized external IT entities accessing the TOE, and human users sending or receiving information through the TOE using FTP or Telnet.

FTP_ITC.1 requires communication with external authorized IT entities to be performed over a secure channel that provides assured identification of its end points. FTP_TRP.1 requires use of a trusted path between the TSF and local users that provides assured identification of its end points for all administration of the TOE.

Taken together, these SFRs ensure that the I&A objective is upheld for all access to TOE functions, and for a defined subset of services that are passed through the TOE.

Note that the O.IDAUTH objective is coordinated with the objective for the IT environment OE.IDAUTH that has been defined to allow the use of non-TOE authentication components such as RADIUS servers. This is compatible with [PD-0115], which suggests that O.IDAUTH and its accompanying/mapped SFRs, FIA_UID.2 and FIA_UAU.5 should be considered as objectives and requirements for the environment.

O.SINUSE *The TOE must prevent the reuse of authentication data for users attempting to authenticate to the TOE from a connected network.*

FIA_ATD.1 exists to provide users with attributes to distinguish one user from another.

FIA_UAU.5 requires that single-use authentication be used appropriately in all attempts to authenticate at the TOE, using the following mechanisms: SIC, IKE, TLS and/or a single-use password. FCS_CKM.2(2) defines the authentication and key distribution protocol to be used for SIC and TLS-based user authentication, and FCS_CKM.2(1) describes the requirement for IKE authentication.

Cryptographic algorithms used for supporting the single-use authentication implementation are compatible with NIAP PD-0105:

- FCS_COP.1(4) defines the use of HMAC-SHA-1 as the keyed hash function;
- FCS_COP.1(5) defines the use of SHA-1 for secure hash computation;
- FCS_COP.1(6) defines the cryptographic algorithm used for authentication with digital signatures;
- FCS_COP.1(7) defines the requirements for Diffie-Hellman key exchange.

O.MEDIAT ***The TOE must mediate the flow of all information between clients and servers located on internal and external networks governed by the TOE, disallowing passage of non-conformant protocols and ensuring that residual information from a previous information flow is not transmitted in any way.***

FDP_IFC.1(1), FDP_IFC.1(2) and FDP_IFC.1(3) identify information flows that must be mediated using unauthenticated application-level proxies, authenticated proxies, and traffic filtering, respectively. Together, these information flows cover any traffic flowing through the TOE. FDP_IFF.1(1), FDP_IFF.1(2) and FDP_IFF.1(3) identify the information security attributes that are used for information flow control, and the information flow control policies to be applied to each information flow. Protocols that do not conform to these rules are disallowed. For the protocols HTTP, SMTP, Telnet and FTP, requests that do not conform to the protocol specifications are rejected.

FMT_MSA.3 ensures that there is a default deny policy for the information flow control security rules. FMT_MSA.1(1), FMT_MSA.1(2), FMT_MSA.1(3) and FMT_MSA.1(4) ensure that the ability to manage the information security attributes that are used for information flow control is restricted to authorized administrators.

FDP_RIP.2 ensures that neither information that had flowed through the TOE nor any TOE internal data are used when padding is used by the TOE for information flows.

O.SECSTA ***Upon initial start-up of the TOE or recovery from an interruption in TOE service, the TOE must not compromise its resources or those of any connected network.***

FMT_MSA.3 ensures that there is a default deny policy for the information flow control security rules, so that resources of any connected network are not compromised upon initial start-up. FMT_MSA.1(1), FMT_MSA.1(2), FMT_MSA.1(3) and FMT_MSA.1(4) ensure that the TSF restricts from TOE start-up the ability to manage the security attributes that influence the enforcement of the information flow control policies, to the authorized administrator.

FAU_STG.2 ensures that the audit trail is always (i.e., from initial start-up) protected from tampering, and that all stored audit records will be maintained after a recovery from an interruption in TOE service. FAU_STG.4 ensures that the authorized administrator will be able to take care of the audit trail if it should become full and resources will not be compromised upon recovery. This component also ensures that no other auditable events as defined in FAU_GEN.1 occur. Thus the authorized administrator is permitted to perform potentially auditable actions though these events will not be recorded until the audit trail is restored to a non-full status.

FMT_MOF.1(1) requires that the TSF restricts the ability of the TOE start up and shut down operation and single-use authentication function (described in FIA_UAU.5) to the authorized administrator. FMT_MOF.1 (2) was to ensure the TSF restricts the ability to modify the behavior of functions such as audit trail management, back and restore for

TSF data, and communication of authorized external IT entities with the TOE to an authorized administrator.

FPT_RVM.1 ensures that the TSF enforcement functions are always invoked.

FPT_AMT.1 and FPT_TST.1 are introduced to require a suite of tests to be run during initial start-up and periodically during normal operation to demonstrate the correct operation of the underlying abstract machine and cryptographic module, and to provide authorized users with the capability to verify the integrity of policy files and stored TSF executable code.

O.ENCRYP ***The TOE must protect the confidentiality of its dialogue with an authorized administrator through encryption, if the TOE allows administration to occur remotely from a connected network.***

FCS_COP.1(1) ensures that if the TOE does support authorized administrators to communicate with the TOE remotely from an internal or external network that Triple DES is used to encrypt such traffic. This component is necessitated by the postulated threat environment.

O.SELPRO ***The TOE must protect itself against attempts by unauthorized users to bypass, deactivate, or tamper with TOE security functions.***

FPT_SEP.1 ensures that the TSF have a domain of execution that is separate and that cannot be violated by unauthorized users. FPT_RVM.1 ensures that the TSF are always invoked.

FPT_AMT.1 and FPT_TST.1 are introduced to require a suite of tests to be run during initial start-up and periodically during normal operation to demonstrate the correct operation of the underlying abstract machine and cryptographic module, and to provide authorized users with the capability to verify the integrity of policy files and stored TSF executable code.

FAU_STG.2 is chosen to ensure that the audit trail is protected from tampering, as well as guarantee the availability of the audit data in the event of storage exhaustion, failure or attack. FAU_STG.4 ensures that the authorized administrator will be able to take care of the audit trail if it should become full and resources will not be compromised upon recovery. This component also ensures that no other auditable events as defined in FAU_GEN.1 occur. Thus the authorized administrator is permitted to perform potentially auditable actions though these events will not be recorded until the audit trail is restored to a non-full status.

IDS_STG(EXP).1 requires the IDS System to protect the System data from any modification and unauthorized deletion, as well as guarantee the availability of the data in the event of storage exhaustion, failure or attack. FMT_MOF.1(3) prevents unauthorized users from modifying IDS System data collection, analysis and reaction functions.

FPT_ITT.1 was introduced to protect communication between distributed parts of the TOE (i.e. SmartCenter Server to appliance management traffic). FTP_TRP.1 provides the administrator with a trusted path between the Management GUI and the SmartCenter Server. FCS_CKM.2(2), FCS_COP.1(2) and FCS_COP.1(5) support these requirements by providing key distribution, encryption and decryption, and secure hash computation, respectively. FMT_MOF.1(5) prevents unauthorized users from enabling SIC to an unauthorized external IT entity.

O.AUDREC ***The TOE must provide a means to record a readable audit trail of security-related events, with accurate dates and times, and a means to search and sort the audit trail based on relevant attributes.***

FAU_GEN.1 outlines what data must be included in audit records and what security-related events must be audited. FAU_SEL.1 provides the capability to select which security-relevant events to audit. FPT_STM.1 supports audit generation by ensuring that the TSF can provide reliable time stamps for audit records.

FAU_SAR.1 ensures that the audit trail is understandable. FAU_SAR.3 ensures that searches and sorts can be performed on the audit trail.

FAU_STG.4 ensures that loss of collected data is prevented.

O.ACCOUN *The TOE must provide user accountability for information flows through the TOE and for authorized administrator use of security functions related to audit.*

FIA_UID.2 ensures that before anything occurs on behalf of a user, the user's identity is identified to the TOE. FIA_USB.1 determines the rules for associating the user identity which is associated with auditable events with a subject acting on behalf of the user.

FAU_GEN.1 outlines what data must be included in audit records and what events must be audited.

FAU_GEN.2 is used in addition to FAU_GEN.1 to address the requirement of accountability of auditable events at the level of individual user identity.

O.SECFUN ***The TOE must provide functionality that enables an authorized administrator to use the TOE security functions, and must ensure that only authorized administrators are able to access such functionality.***

FIA_ATD.1 requires that the TOE maintain for each human user his or her association with an authorized administrator role defined in FMT_SMR.1. FIA_UID.2 and FIA_UAU.1 require administrators to be identified and authenticated before receiving access to the TOE. FTP_TRP.1 establishes a trusted path that is used for administration of the TOE. FAU_GEN.1 specifies management events that must be audited.

FMT_SMF.1 requires that the TOE provide functionality that enables an authorized administrator to use the TOE security functions listed in Table 5-3. FMT_MOF.1(1), FMT_MOF.1(2), FMT_MOF.1(3), FMT_MOF.1(4), FMT_MOF.1(5), FMT_MSA.1(1), FMT_MSA.1(2), FMT_MSA.1(3), FMT_MSA.1(4) , FMT_MSA.1(5) and FMT_MTD.1(4) restrict the use of these management functions to authorized administrator roles, as specified in Table 5-3.

FMT_MSA.3 requires that the TSF allow the authorized administrator to provide alternative initial values to override the default values when an object or information is created.

FAU_SEL.1, FAU_SAR.1, FAU_SAR.3 and require the TOE to provide capabilities for managing the set of audited events, and to provide the ability to review the audit trail. FAU_SAR.2 restricts audit record review to authorized administrators. FAU_STG.2 prevent unauthorized deletion or modification of the audit trail.

IDS_RDR(EXP).1 provides the ability for authorized administrators to view all IDS System data collected and produced.

FAU_STG.4 ensures that the authorized administrator will be able to take care of the audit trail if it should become full and resources will not be compromised upon recovery. This component also ensures that no other auditable events occur. Thus the authorized administrator is permitted to perform potentially auditable actions though these events will not be recorded until the audit trail is restored to a non-full status. IDS_STG(EXP).2 requires equivalent functionality for IDS System data.

FPT_TST.1 provides authorized users with the capabilities to verify the integrity of policy files as well as stored TSF executable code.

O.LIMEXT ***The TOE must provide the means for an authorized administrator to control and limit access to TOE security functions by an authorized external IT entity.***

FMT_SMF.1 defines a management function for controlling communication with authorized external IT entities.

The following requirements restrict management functions that can be used to modify the behavior of the communication with authorized external IT entities to the authorized administrator:

- FMT_MOF.1 (2) restricts the ability to modify the behavior of the communication of authorized external IT entities with the TOE;
- FMT_MOF.1 (1) restricts management of the single-use authentication function for authorized external IT entities (described in FIA_UAU.5).

O.EAL ***The TOE must be methodically tested and shown to be resistant to attackers possessing moderate attack potential.***

This objective was mapped to Security Assurance Requirements – see section 8.2.3 below.

O.IDSENS ***The Sensor must collect and store information about all events that are indicative of inappropriate activity that may have resulted from misuse, access, or malicious activity of IT System assets and the IDS.***

IDS_SDC(EXP).1 requires the IDS System to be able to collect and store information indicative of inappropriate activity that may have resulted from misuse, access, or malicious activity. For this TOE, the IDS Sensor is integrated with the TOE's audit recording functionality.

O.IDANLZ ***The Analyzer must accept data from IDS Sensors or IDS Scanners and then apply analytical processes and information to derive conclusions about intrusions (past, present, or future).***

IDS_ANL(EXP).1 requires the IDS System to perform signature-based intrusion analysis and generate conclusions. This requirement is supported by FAU_SAA.3 which requires the TOE to be able to match network traffic mediated by the TOE against signature events represented as Stateful Inspection rules.

O.RESPON ***The TOE must respond appropriately to analytical conclusions.***

IDS_RCT(EXP).1 requires the TOE to respond accordingly in the event an intrusion is detected.

O.OFLOWS ***The TOE must appropriately handle potential audit and IDS System data storage overflows.***

FAU_STG.2 ensures that stored audit records are protected from unauthorized deletion, and that all stored audit records will be maintained in the event of audit storage exhaustion. When an audit storage failure is imminent, FAU_STG.3 requires the TSF to send an alarm to allow the administrator to take appropriate action. When the audit trail is full, FAU_STG.4 requires the TSF to prevent auditable events (except those taken by the authorized administrator), limit the number of audit records lost and send an alarm.

IDS_STG(EXP).1 and IDS_STG(EXP).2 define equivalent requirements to FAU_STG.2 and FAU_STG.4, respectively, pertaining to IDS System data overflows.

O.INTEGR ***The TOE must ensure the integrity of all audit and IDS System data.***

FAU_STG.2 and IDS_STG(EXP).1 ensure that stored audit records and IDS System data are protected from unauthorized modification or deletion, and that all stored audit records will be maintained in the event of audit storage exhaustion, failure or attack.

FMT_MTD.1(3) ensures that only authorized administrators may query or add audit and System data.

O.VPN ***The TOE must be able to protect the integrity and confidentiality of data transmitted to a peer authorized external IT entity via encryption and provide authentication for such data. Upon receipt of data from a peer authorized external IT entity, the TOE must be able to decrypt the data and verify that the received data accurately represents the data that was originally transmitted.***

FDP_UIT.1 and FDP_UCT.1 establish requirements for the protection of the integrity and confidentiality of data transmitted to a peer authorized external IT entity. FTP_ITC.1 supports these requirements by requiring a trusted channel to be used for VPN traffic that provides assured identification of its end points and protection of the communicated data from modification or disclosure.

FDP_IFC.1(3) and FDP_IFF.1(3) define the information flow control policy that encrypts outgoing VPN traffic and decrypts incoming VPN traffic, according to rules creates by the authorized administrator. Management of these rules is restricted to the authorized administrator by FMT_MSA.1(5).

The following requirements define the cryptographic algorithms and protocols that must be used to meet this objective:

- FCS_CKM.2(1) requires the use of IKE cryptographic key distribution for IPSec VPNs;
- FCS_COP.1(3) requires support for Triple DES and AES for encryption and decryption of IPSec VPN traffic;
- FCS_CKM.2(2) requires the use of TLSv1.0 cryptographic key distribution for SSL VPNs;
- FCS_COP.1(2) requires support for Triple DES for encryption and decryption of SSL VPN traffic;
- FCS_COP.1(4), FCS_COP.1(5), FCS_COP.1(6) and FCS_COP.1(7) define requirements for HMAC-SHA-1, SHA-1, RSA and Diffie Hellman, respectively.

8.2.2. SFRs for the IT Environment Rationale

Table 8-5 maps SFRs to the defined security objectives for the IT environment. The table demonstrates that each security objective for the IT environment is met by one or more SFRs, and that each SFR for the IT environment meets at least one security objective. This is followed by appropriate explanatory text that provides further justification that the mapped SFRs are suitable to meet the security objectives for the IT environment.

Table 8-5 – IT Environment Security Objective to Functional Component Mapping

	OE.IDAUTH	OE.VPN
FDP_UCT.1(Env)		✓
FDP_UIT.1(Env)		✓
FIA_UAU.5(Env)	✓	
FTP_ITC.1(Env)		✓

OE.IDAUTH ***The IT environment must support the unique identification and authentication of the claimed identity of all users, before a user is granted access to TOE functions or, for certain specified services, to a connected network.***

FIA_UAU.5(Env) is a supporting SFR to FIA_UAU.5. It requires that the IT environment be able to provide an authentication server that validates single-use passwords for a given user identity, to support the TOE in authenticating human users sending or receiving information through the TOE where an administrator configures authentication via a single-use password mechanism. The TOE itself does not provide a single-use password validation capability.

For certificate-based authentication, FIA_UAU.5(Env) requires a certificate authority in the environment, if relied-on by the TOE, to generate and distribute certificates and revocation information in a secure manner.

OE.VPN ***Peer external IT entities must be able to protect the integrity and confidentiality of data transmitted to the TOE via encryption and provide authentication for such data. Upon receipt of data from the TOE, the peer external IT entity must be able to decrypt the data and verify that the received data accurately represents the data that was originally transmitted.***

FDP_UCT.1(Env), FDP_UIT.1(Env) and FTP_ITC.1(Env) are requirements for the IT environment that correspond to TOE requirements FDP_UCT.1, FDP_UIT.1 and FTP_ITC.1, respectively. They ensure that IPSec VPN peers implement a coordinated security policy with the TOE in order to protect traffic between the TOE and its VPN peers from unauthorized disclosure or modification.

8.2.3. Security Assurance Requirements Rationale

The level of assurance chosen for this ST is that of Evaluation Assurance Level (EAL) 4, as defined in [CC] Part 3, augmented with the [CC] Part 3 component ALC_FLR.3 and AVA_VLA.3. This set of requirements serves to meet O.EAL, as described below.

This PP claims PP compliance. The Firewall PPs define the minimum security requirements for firewalls in a moderate risk environment as EAL 2 augmented. The IDS System PP assumes that the IDS System will be protected from hostile attack, and therefore requires a lower level of assurance, EAL 2 with no augmentation.

Table 8-6 tabulates each claimed PP with the security assurance augmentations for that PP above its base EAL. Several assurance components from EAL 4 have been required by the firewall PPs to provide appropriate assurance for the expected application of the product. EALs are predefined packages of assurance requirements that have been determined by the CC to provide a balanced level of assurance. EAL 4 has therefore been selected by the evaluation sponsors as an appropriate base EAL for this ST that is consistent with the PP assurance requirements.

Table 8-6- Assurance Requirements for Claimed PPs

Claimed PP	Base EAL	Augmentations	EAL where augmentation appears
[APP-PP] [TFF-PP]	EAL2	ADV_HLD.2	EAL 3
		ADV_IMP.1	EAL 4
		ADV_LLD.1	EAL 4
		ALC_TAT.1	EAL 4
		AVA_VLA.3	EAL 5
[IDSSPP]	EAL2	None	

EAL 4 ensures that the product has been methodically designed, tested, and reviewed with maximum assurance from positive security engineering based on good commercial development practices. It is applicable in those circumstances where developers or users require a moderate to high level of independently assured security.

To ensure the security of Mission-Critical Categories of information, not only must vulnerability analysis by the developer be performed, but an evaluator must perform independent penetration testing to determine that the TOE is resistant to penetration attacks performed by attackers possessing a moderate attack potential. This level of testing is required in this ST by AVA_VLA.3, as required by the firewall PPs.

In addition, the assurance requirements have been augmented with ALC_FLR.3 (Systematic flaw remediation) to provide assurance that the TOE will be maintained and supported in the future, requiring the TOE developer to track and correct flaws in the TOE, and providing guidance to TOE users for how to submit security flaw reports to the developer, and how to register themselves with the developer so that they may receive these corrective fixes.

8.2.4. Extended Requirements Rationale

This ST includes the following explicitly stated functional requirements, all taken from [IDSSPP]. These requirements were included in the ST in order to comply with the PP. Justification for these explicitly stated functional requirements is as in [IDSSPP].

Table 8-7- Explicitly Stated Security Functional Requirements

Extended Component	
IDS_SDC(EXP).1	System Data Collection
IDS_ANL(EXP).1	Analyser analysis
IDS_RCT(EXP).1	Analyser react
IDS_RDR(EXP).1	Restricted Data Review
IDS_STG(EXP).1	Guarantee of System Data Availability
IDS_STG(EXP).2	Prevention of System data loss

8.2.5. Dependency Rationale

Table 8-8 depicts the satisfaction of all security requirement dependencies. For each security requirement included in the ST, the CC dependencies are identified in the column "CC dependency", and the satisfied dependencies are identified in the "ST dependency" column. Iterated components are identified to help determine exactly which specific iteration is dependent on which SFR or SAR.

Note: none of the explicitly stated requirements in this ST have defined dependencies.

Dependencies that are satisfied by hierarchically higher or alternative components are given in **boldface**, and explained in the "Dependency description" column.

Table 8-8- Security Requirements Dependency Mapping

SFR	CC dependency	ST dependency	Dependency description
FAU_GEN.1	FPT_STM.1	FPT_STM.1	Audit dependency on secure time.
FAU_GEN.2	FAU_GEN.1, FIA_UID.1	FAU_GEN.1, **FIA_UID.2**	FIA_UID.2 is hierarchical to FIA_UID.1 so it can be used to satisfy the dependency
FAU_SAA.3	None		
FAU_SAR.1	FAU_GEN.1	FAU_GEN.1	Audit review dependency on audit generation.
FAU_SAR.2	FAU_SAR.1	FAU_SAR.1	
FAU_SAR.3	FAU_SAR.1	FAU_SAR.1	
FAU_SEL.1	FAU_GEN.1, FMT_MTD.1	FMT_GEN.1, FMT_MTD.1(3)	Selective audit dependency on audit generation and on management of audit data.
FAU_STG.2	FAU_GEN.1	FAU_GEN.1	
FAU_STG.3	FAU_STG.1	**FAU_STG.2**	FAU_STG.2 is hierarchical to FAU_STG.1 so it can be used to satisfy the dependency.
FAU_STG.4	FAU_STG.1	**FAU_STG.2**	FAU_STG.2 is hierarchical to FAU_STG.1 so it can be used to satisfy the dependency.
FCS_CKM.2(1)	[FCS_ITC.1 or FCS_CKM.1], FCS_CKM.4, FMT_MSA.2	**None**	Justification for excluding FCS_ITC.1, FCS_CKM.1, FCS_CKM.4 and FMT_MSA.2 is as given in [APP-PP] and [TFF-PP].
FCS_CKM.2(2)			
FCS_COP.1(1)	[FCS_ITC.1 or FCS_CKM.1],	**None**	Justification for excluding FCS_ITC.1, FCS_CKM.1,
FCS_COP.1(2)			

SFR	CC dependency	ST dependency	Dependency description
FCS_COP.1(3)	FCS_CKM.4, FMT_MSA.2		FCS_CKM.4 and FMT_MSA.2 is as given in [APP-PP] and [TFF-PP].
FCS_COP.1(4)			
FCS_COP.1(5)			
FCS_COP.1(6)			
FCS_COP.1(7)			
FDP_IFC.1(1)	FDP_IFF.1	FDP_IFF.1(1)	Dependent components.
FDP_IFC.1(2)		FDP_IFF.1(2)	
FDP_IFC.1(3)		FDP_IFF.1(3)	
FDP_IFF.1(1)	FDP_IFC.1, FMT_MSA.3	FDP_IFC.1(1), FMT_MSA.3	Dependency on SFP definition and on default or initial values for information flow security attributes.
FDP_IFF.1(2)		FDP_IFC.1(2) , FMT_MSA.3	
FDP_IFF.1(3)		FDP_IFC.1(3) , FMT_MSA.3	
FDP_RIP.2	None		
FDP_UCT.1	[FTP_ITC.1 or FTP_TRP.1] [FDP_ACC.1 or FDP_IFC.1]	FTP_ITC.1, FDP_IFC.1(3)	Dependency on inter-TSF trusted channel and on the TRAFFIC FILTER SFP.
FDP_UIT.1			
FDP_UCT.1(Env)	[FTP_ITC.1 or FTP_TRP.1] [FDP_ACC.1 or FDP_IFC.1]	FTP_ITC.1(Env), FDP_IFC.1(3)	Dependency on inter-TSF trusted channel and on the TRAFFIC FILTER SFP.
FDP_UIT.1(Env)			
FIA_ATD.1	None		
FIA_UAU.1	FIA_UID.1	**FID_UID.2**	FIA_UID.2 is hierarchical to FIA_UID.1 so it can be used to satisfy the dependency.
FIA_UAU.5	None		
FIA_UAU.5(Env)	None		
FIA_UID.2	None		
FIA_USB.1	FIA_ATD.1	FIA_ATD.1	Dependency of association of user security attributes with subjects on the definition of these attributes.
FMT_MOF.1(1)	FMT_SMF.1,	FMT_SMF.1,	Management restrictions

SFR	CC dependency	ST dependency	Dependency description
FMT_MOF.1(2)	FMT_SMR.1	FMT_SMR.1	dependency on management functions and administrator roles
FMT_MOF.1(3)			
FMT_MOF.1(4)			
FMT_MOF.1(5)			
FMT_MSA.1(1)	[FDP_ACC.1 or FDP_IFC.1], FMT_SMF.1, FMT_SMR.1	FDP_IFC.1(1), FDP_IFC.1(3), FMT_SMF.1, FMT_SMR.1	Management of security attributes dependency on an information flow control policy that uses these attributes, on management functions being available, and on appropriate security roles.
FMT_MSA.1(2)		FDP_IFC.1(2), FMT_SMF.1, FMT_SMR.1	
FMT_MSA.1(3)		FDP_IFC.1(1), FDP_IFC.1(3), FMT_SMF.1, FMT_SMR.1	
FMT_MSA.1(4)		FDP_IFC.1(2), FMT_SMF.1, FMT_SMR.1	
FMT_MSA.1(5)		FDP_IFC.1(1), FDP_IFC.1(2), FDP_IFC.1(3), FMT_SMF.1, FMT_SMR.1	
FMT_MSA.3	FMT_MSA.1, FMT_SMR.1	FMT_MSA.1(1), FMT_MSA.1(2), FMT_MSA.1(3), FMT_MSA.1(4), FMT_MSA.1(5), FMT_SMR.1	Static attribute initialization dependency on attribute management and security roles.
FMT_MTD.1(1)	FMT_SMF.1, FMT_SMR.1	FMT_SMF.1, FMT_SMR.1	Management restriction dependency on management functions and security roles.
FMT_MTD.1(2)			
FMT_MTD.1(3)			
FMT_MTD.1(4)			
FMT_SMF.1	None		
FMT_SMR.1	FIA_UID.1	**FIA_UID.2**	FIA_UID.2 is hierarchical to FIA_UID.1 so it can be used to satisfy the dependency.

SFR	CC dependency	ST dependency	Dependency description
FPT_AMT.1	None		
FPT_ITT.1	None		
FPT_RVM.1	None		
FPT_SEP.1	None		
FPT_STM.1	None		
FPT_TST.1	FPT_AMT.1	FPT_AMT.1	Self-test dependency on abstract machine testing.
FTP_ITC.1	None		
FTP_ITC.1(Env)	None		
FTP_TRP.1	None		
IDS_SDC(EXP).1	None		
IDS_ANL(EXP).1	None		
IDS_RCT(EXP).1	None		
IDS_RDR(EXP).1	None		
IDS_STG(EXP).1	None		
IDS_STG(EXP).2	None		
ACM_AUT.1	ACM_CAP.3	**ACM_CAP.4**	Consistent with EAL 4
ACM_CAP.4	ALC_DVS.1	ALC_DVS.1	Consistent with EAL 4
ACM_SCP.2	ACM_CAP.3	**ACM_CAP.4**	Consistent with EAL 4
ADO_DEL.2	ACM_CAP.3	**ACM_CAP.4**	Consistent with EAL 4
ADO_IGS.1	AGD_ADM.1	AGD_ADM.1	Consistent with EAL 4
ADV_FSP.2	ADV_RCR.1	ADV_RCR.1	Consistent with EAL 4
ADV_HLD.2	ADV_FSP.1, ADV_RCR.1	**ADV_FSP.2**, ADV_RCR.1	Consistent with EAL 4
ADV_IMP.1	ADV_LLD.1, ADV_RCR.1, ALC_TAT.1	ADV_LLD.1, ADV_RCR.1, ALC_TAT.1	Consistent with EAL 4
ADV_LLD.1	ADV_HLD.2, ADV_RCR.1	ADV_HLD.2, ADV_RCR.1	Consistent with EAL 4
ADV_RCR.1	None defined explicitly	ADV_FSP.2, ADV_HLD.2, ADV_LLD.1,	Correspondence demonstration dependency on the functional specification, the high-level design,

SFR	CC dependency	ST dependency	Dependency description
		ADV_IMP.1	the low-level design and the ADV_IMP.1 selected subset of the implementation representation.
ADV_SPM.1	ADV_FSP.1	**ADV_FSP.2**	Consistent with EAL 4
AGD_ADM.1	ADV_FSP.1	**ADV_FSP.2**	Consistent with EAL 4
AGD_USR.1	ADV_FSP.1	**ADV_FSP.2**	Consistent with EAL 4
ALC_DVS.1	None		
ALC_FLR.3	None		
ALC_LCD.1	None		
ALC_TAT.1	ADV_IMP.1	ADV_IMP.1	Consistent with EAL 4
ATE_COV.2	ADV_FSP.1, ATE_FUN.1	ADV_FSP.1, ATE_FUN.1	Consistent with EAL 4
ATE_DPT.1	ADV_HLD.1, ATE_FUN.1	**ADV_HLD.2**, ATE_FUN.1	Consistent with EAL 4
ATE_FUN.1	None		
ATE_IND.2	ADV_FSP.1, AGD_ADM.1, AGD_USR.1, ATE_FUN.1	**ADV_FSP.2**, AGD_ADM.1, AGD_USR.1, ATE_FUN.1	Consistent with EAL 4
AVA_MSU.2	ADO_IGS.1, ADV_FSP.1, AGD_ADM.1, AGD_USR.1	ADO_IGS.1, **ADV_FSP.2**, AGD_ADM.1, AGD_USR.1	Consistent with EAL 4
AVA_SOF.1	ADV_FSP.1, ADV_HLD.1	**ADV_FSP.2**, **ADV_HLD.2**	Consistent with EAL 4.
AVA_VLA.3	ADV_FSP.1, ADV_HLD.2, ADV_IMP.1, ADV_LLD.1, AGD_ADM.1, AGD_USR.1	**ADV_FSP.2**, ADV_HLD.2, ADV_IMP.1, ADV_LLD.1, AGD_ADM.1, AGD_USR.1	Augmentation of EAL 4

8.2.6. Internal Consistency and Mutual Support

This section demonstrates that the stated security requirements together form a mutually supportive and internally consistent whole.

No operations have been performed on SARs. A base evaluation assurance level of EAL 4 was selected as described in section 8.2.3 to ensure the internal consistency and mutual support of the SARs in this ST. Section 8.2.3 also provides justification for any augmentations above EAL 4.

The dependency analysis in section 8.2.5 demonstrates that mutual support interactions defined in [CC] Part 2 and Part 3 have been correctly resolved: by definition, if requirement A has a dependency on requirement B, B supports A.

Because this ST claims compliance to validated PPs, justification has been provided in each PP for the internal consistency and mutual support of its claimed requirements. This analysis therefore focuses on the interactions between the requirements of the claimed PPs, and on requirements introduced in this ST that are not restated from a validated PP, including VPN-related SFRs and other supporting SFRs.

8.2.6.1. Consistency Analysis

The two firewall PPs, [APP-PP] and [TFF-PP], were constructed to be mutually consistent. Both use the same terminology, and almost identical requirements. As identified in Table 5-1 column 3, the only mismatch in requirements between the two PPs relates to the information flow control and corresponding management requirements (any requirement traced to "Both" or "All" appears in both PPs). In order to maintain consistency between the differing information flow control requirements, the [TFF-PP] requirements were renamed as described in the application note in section 5.1.

The [IDSSPP] does not introduce any significant inconsistencies with the firewall PPs. Many of its requirements are also specified in the firewall PPs. Specific IDS functionality was introduced using explicitly stated extended requirements in the IDS(EXP) class, thereby minimizing the interaction between IDS and firewall requirement components.

The selection and assignment operations on the IDS_SDC(EXP).1 component were performed in a manner that binds the IDS System Sensor functionality to network traffic-related events. The selection taken for IDS System Analyzer functionality refers to signature analysis. The binding of IDS and firewall functionality is supported by the introduction in this ST of the FAU_SAA.3 component, clarifying that signatures are represented in the product as Stateful Inspection rules, which are compared against network traffic mediated by the TOE.

Authentication requirements are set forth in the [IDSSPP] using the FIA_UAU.1 component, and the FIA_UAU.5 component for the firewall PPs. FIA_UAU.1 describes the TSF-mediated actions that are permitted prior to the TSF authenticating the user. The assignment for this component was made to include information flows that are not authenticated exclusively by the TSF, to prevent a possible inconsistency with FIA_UAU.5.

A minor inconsistency that has been encountered when merging [IDSSPP] requirements in addition to the firewall PP requirements was with FMT_SMR.1: [IDSSPP] requires at least two administrator roles to be defined to differentiate between management of the platform and of the IDS functionality, whereas the firewall PPs define only one administrator role. This inconsistency was resolved by requiring two roles: an authorized administrator, and an authorized audit administrator. The audit administrator is responsible for reviewing audit and IDS System data, but is not authorized to modify the information flow control rules or other non audit or IDS-related functionality.

The TOE's VPN security functionality was incorporated by adding requirements for inter-TSF integrity and confidentiality, supported by requirements for inter-TSF trusted channels and associated requirements in the FCS class. (Note that these requirements are unrelated to the corresponding ITA, ITC and ITI requirements mentioned in [IDSSPP]; [PD-0097] explains that these requirements were erroneously replicated into the IDS System PP, and must be removed.)

The VPN requirement was integrated with the traffic filtering functionality defined in FDP_IFF.1(3), so as to be able to apply to all information flows through the TOE, with no compromise of any firewall or IDS functionality.

The audit generation and management requirements have been expanded to cover all SFRs specified in this ST.

All other security requirements added in this ST have been introduced to either satisfy [CC] dependencies or to provide additional support for one or more of the stated requirements, and are consistent with all other requirements in the ST.

8.2.6.2. Mutual Support Analysis

Mutual support is shown through consideration of the interactions between the SFRs. The security requirements work mutually so that each primary SFR is protected against bypassing, tampering, and deactivation by other SFRs.

The *primary* SFRs are the requirements that address the primary objectives, namely O.IDAUTH, O.MEDIAT, O.ENCRYP, O.AUDREC, O.ACCOUN, O.IDSENS, O.IDANLZ, O.RESPON and O.VPN. The SFRs directly addressing these objectives are described above in the Security Functional Requirements Rationale.

In general, the following mutual support interactions can be seen to exist between the primary objectives:

- The TOE's VPN functionality supports single-use authentication and encryption of administration sessions;
- Audit supports IDS recording;
- IDS supports traffic filtering and vice versa, as well as self-protection;
- The TOE's medium-robustness firewall self-protection capability protects the IDS System against bypass, tampering, and deactivation.

In addition, the following SFRs have been added to the ST, in addition to the SFRs defined in the claimed PPs and the VPN-related SFRs, to provide additional support for the primary SFRs:

Table 8-9 – Additional supporting SFRs introduced in this ST

Functional Component	Support Type	Inclusion Rationale
FAU_GEN.2	Prevention of bypass	Ensures that user identity is recorded for all applicable auditable events. The inclusion of this component is called for (normative *should*) in [CC] Part2, Annex C.2, paragraph 564.
FAU_SAA.3	Prevention of bypass	IDS analysis is applied to all traffic flowing through the TOE
FAU_STG.3	Detection of tampering	Allows an administrator to receive an alarm when audit storage falls below an administrator-defined threshold.
FCS_CKM.2(1) and FCS_CKM.2(2)	Cryptographic support	Cryptographic key distribution
FCS_COP.1(1) through FCS_COP.1(7)	Cryptographic support	Cryptographic operations
FIA_USB.1	Prevention of bypass	Determines the rules for association of user security attributes with subjects acting on the behalf of users. This requirement is used to determine the relationship between authenticated and unauthenticated identity.
FPT_AMT.1 and FPT_TST.1	Detection of tampering or de-activation	Self-test capabilities support the TOE's self-protection capabilities
FPT_ITT.1	Prevention of tampering	Per [PD-0097], if the TOE of an IDS System is a distributed TOE, FPT_ITT.1 must be included to protect those communications.
FTP_TRP.1	Prevention of bypass	Supports the single-use authentication requirement for remote administrators by countering network hijacking, MITM and similar attacks.

8.2.7. Strength of Function (SOF) Rationale

The TOE strength of function is claimed to be ‘SOF-medium’ or higher, in accordance with the strength of function requirements of both firewall PPs.

8.3. TOE Summary Specification Rationale

This section in conjunction with Section 6, the TOE Summary Specification, provides evidence that the security functions are suitable to meet the TOE security functional requirements (SFRs) and security assurance requirements (SARs).

The security requirements are mutually supportive and consistent, as shown above in section 8.2.6.

8.3.1. TOE Security Functions Rationale

The collection of security functions work together to provide all of the security functional requirements as indicated in Table 8-10. All points where this could cause conflict were examined and this was not the case. It is also evident from an inspection of the tables that the security functions described in the TSS are all necessary to address the required security functionality of the TSF.

Table 8-10- TOE Summary Specification Rationale Mapping

	Stateful Inspection	Security Servers	VPN	Audit	Management	SIC	I&A	TSF Protection
FAU_GEN.1				✓				
FAU_GEN.2				✓				
FAU_SAA.3	✓							
FAU_SAR.1				✓				
FAU_SAR.2				✓				
FAU_SAR.3				✓				
FAU_SEL.1				✓				
FAU_STG.2				✓				
FAU_STG.3				✓				
FAU_STG.4				✓				
FCS_CKM.2(1)			✓					
FCS_CKM.2(2)			✓			✓		
FCS_COP.1(1)			✓					
FCS_COP.1(2)			✓			✓		
FCS_COP.1(3)			✓					
FCS_COP.1(4)			✓					
FCS_COP.1(5)			✓			✓		

	Stateful Inspection	Security Servers	VPN	Audit	Management	SIC	I&A	TSF Protection
FCS_COP.1(6)			✓			✓		
FCS_COP.1(7)			✓					
FDP_IFC.1(1)	✓	✓						
FDP_IFC.1(2)	✓	✓						
FDP_IFC.1(3)	✓							
FDP_IFF.1(1)	✓	✓						
FDP_IFF.1(2)	✓	✓						
FDP_IFF.1(3)	✓		✓					
FDP_RIP.2	✓							
FDP_UCT.1			✓					
FDP_UIT.1			✓					
FIA_ATD.1					✓			
FIA_UAU.1							✓	
FIA_UAU.5							✓	
FIA_UID.2							✓	
FIA_USB.1							✓	
FMT_MOF.1(1)					✓			
FMT_MOF.1(2)					✓			
FMT_MOF.1(3)					✓			
FMT_MOF.1(4)					✓			
FMT_MOF.1(5)					✓			
FMT_MSA.1(1)					✓			
FMT_MSA.1(2)					✓			
FMT_MSA.1(3)					✓			
FMT_MSA.1(4)					✓			
FMT_MSA.1(5)					✓			
FMT_MSA.3	✓				✓			
FMT_MTD.1(1)					✓			
FMT_MTD.1(2)					✓			

	Stateful Inspection	Security Servers	VPN	Audit	Management	SIC	I&A	TSF Protection
FMT_MTD.1(3)				✓	✓			
FMT_MTD.1(4)					✓			
FMT_SMF.1					✓			
FMT_SMR.1					✓			
FPT_AMT.1								✓
FPT_ITT.1						✓		
FPT_RVM.1								✓
FPT_SEP.1								✓
FPT_STM.1								✓
FPT_TST.1								✓
FTP_ITC.1			✓					
FTP_TRP.1						✓		
IDS_SDC(EXP).1				✓				
IDS_ANL(EXP).1	✓			✓				
IDS_RCT(EXP).1	✓			✓				
IDS_RDR(EXP).1				✓				
IDS_STG(EXP).1				✓				
IDS_STG(EXP).2				✓				

8.3.2. Assurance Measures Rationale

The assurance measures that correspond to the security assurance requirements are demonstrated in Section 6, and are further explained in the referred documentation. Table 6-5 in particular shows that all SARs are met by appropriate documentation or physical evidence.

8.3.3. Strength of Function Rationale

The only security function for which a strength of function claim is appropriate is Identification and Authentication (I&A), tracing to FIA_UAU.5.

The strength of function analysis provided in the Vulnerability Analysis assurance measure demonstrates that the single-use authenticators described for the External IT Entity Authentication capability meet the SOF-medium strength of function requirement for FIA_UAU.5.

Administrator authentication, TLS and IKE are performed using cryptographic (rather than permutational and/or probabilistic) mechanisms and are therefore not subject to strength of function analysis.

Authentication of human users using single-use passwords is performed with the support of the IT environment, which both generates and validates the passwords.

8.4. PP Claims Rationale

This section is intended to explain any difference between the ST security objectives and requirements and those of any PP to which conformance is claimed.

Chapter 7 describes the method used to tailor PP security objectives and requirements for this ST, and the security objectives and requirements that were incorporated in this ST in addition to the ones taken from the claimed PPs.

The following firewall PP SFRs have been omitted from this ST: FIA_AFL.1 and FMT_MTD.2. FIA_AFL.1 requires that an account lockout mechanism be in place that prevents administrator and external IT entity access after an administrator-defined number of unsuccessful authentication events. In the TOE evaluated configuration, both administrators and external IT entities authenticate to the TOE using certificate-based authentication mechanisms, rather than via password-based authentication. Given the cryptographic key sizes used, a brute-force attack on authentication secrets is infeasible and therefore lockout is irrelevant in this context. FMT_MTD.2 is a management requirement corresponding to FIA_AFL.1. It too is therefore omitted from this ST.

FMT_MTD.1(2) was refined to restrict the setting of the time and date after the TOE is operational. This can be considered more secure than restricting this function to the authorized administrator, and is therefore consistent with the intention of the PP. As a consequence of this refinement, the auditable event in FAU_GEN.1 for an administrator change of the time and date was removed.

The following precedent decisions have been used as guidance for interpreting the claimed PPs:

Table 8-11- References to Guidance on the Interpretation of Claimed PPs

Reference	Affected PPs	Affected SFRs and objectives	Description
[PD-0018]	[APP-PP], [TFF-PP]	FDP_IFF.1	The term "loopback address" is to be used in place of "loopback network"
[PD-0026]	[APP-PP]	FDP_IFF.1	User identity erroneously referenced for UNAUTHENTICATED SFP
[PD-0055]	[APP-PP], [TFF-PP], [IDSSPP]	Objectives for the environment	Additional assumptions are allowed if they do not violate the intent of the PP
[PD-0086]	[APP-PP], [TFF-PP], [IDSSPP]	O.EAL	A TOE can meet its EAL without using probabilistic mechanisms. When no TOE security functions are realized by probabilistic or permutational mechanisms, a SOF claim is not applicable.

Reference	Affected PPs	Affected SFRs and objectives	Description
[PD-0097]	[IDSSPP]	O.EXPORT, FPT_ITA.1, FPT_ITC.1, FPT_ITI.1, FIA_AFL.1	Incorrectly included in the System PP – must be removed from the PP
		FPT_ITT.1	Must be included in a distributed TOE
[PD-0105]	[APP-PP], [TFF-PP]	FIA_UAU.5	IKE authentication is acceptable as "single use"
[PD-0115]	[APP-PP], [TFF-PP]	O.IDAUTH, FIA_UID.2, FIA_UAU.5	Moved to the environment to support use of external authentication servers

Appendix A - TOE Hardware Platforms

A.1. Supported Hardware for Check Point SecurePlatform

The following commodity hardware platforms are included in the evaluated configuration for the security policy enforcement software (appliances) as well as the SmartCenter Server, running the Check Point SecurePlatform NGX R65 (Take 224[48]) with HFA 30 operating system.

The listed platforms support different processor, memory, mass storage, and network controller configurations. The following guidelines should be used for platform selection:

- **CPU**:
  - Single or dual AMD Opteron® processor configurations
  - Single or dual Intel XEON® processor configurations
  - Other processors that are code-compatible with the listed configurations[49]
- **Memory**: a minimum of 256 Mbytes (512 Mbytes recommended)
- **Mass Storage**: a minimum of 4 GBytes
- **Network controllers**: the following adapter families are included:

Chipset	Driver	Included Adapters
Intel® 825xx	e100	Any adapter from the Intel® Pro/100 family
	e1000	Any adapter from the Intel® Pro/1000 or Intel® Pro/10GbE families
		HP Proliant NC61xx, NC71xx, NC310x and NC340x Gigabit Ethernet NICs
Broadcom chipsets	bcm5700	Any adapter from the Broadcom NetXtreme Gigabit Ethernet adapter family
		HP ProLiant NC10xx, NC67xx, NC77xx, NC150x, NC320x, NC324x, NC325x, NC326x Gigabit Ethernet NICs
Marvell Yukon chipsets	sk98lin	Any adapter based on a Marvell Yukon 88E80xx Gigabit Ethernet controller

[48] Take 224 is the NGX R65 software build distributed on the General Availability Check Point VPN-1 Power/UTM installation media described in Section 2.3.2.

[49] Check Point FIPS 140-2 testing was performed on single and dual Intel Xeon and AMD Opteron configurations. FIPS 140-2 Implementation Guidance G.5 allows vendor porting and re-compilation of a validated firmware cryptographic module to a processor configuration that was not included as part of the validation testing, when this does not require source code modifications. The validation status is maintained in this case without re-testing.

- **Platforms**:

Make	Model
Check Point	Integrated Appliance Solution M2, M6, M8, M8T
	UTM-1 450, 1050, 2050
Crossbeam	C2, C6
	C12, C25
Dell	PowerEdge 650, 750, 850, 860
	PowerEdge 1750, 1850, 1950
	PowerEdge 2650, 2850, 2950
	PowerEdge 2970
	PowerEdge SC1425, SC1435
HP	Proliant DL360 G4, G5, G6
	Proliant DL380 G3, G4, G5, G6
	Proliant DL385
	Proliant DL-585 G1
	Proliant ML330 G3
	Proliant ML350 G4, G5
	Proliant ML370 G4, G5
IBM	xSeries 205, 206, 335, 336, 345, 346
	xSeries 306m
	System x3250, System x3450, System x3550
	System x3650, System x3655
	BladeCenter HS/20, HS/21, HS/22, LS/21, LS/22, LS/43
Patriot Technologies	SMARTGig 1U, 2U, CT
Siemens	4YourSafety RX100 Server
	4YourSafety RX300S Server
Sun	SunFire X2100 Server, X2100 M2 Server
	SunFire X2200 M2 Server
	SunFire X4100 Server
	SunFire X4200 Server
SuperMicro	6023P-8R
Toshiba	Magnia 2200R

A.2. Supported Check Point Security Appliances

The following Check Point security appliance models are included in the evaluated configuration for the security policy enforcement software (gateways):

- Power-1 5070
- Power-1 9070
- UTM-1 130
- UTM-1 270
- UTM-1 570
- UTM-1 1070
- UTM-1 2070
- UTM-1 2070-E
- UTM-1 3070

These appliances run Check Point VPN-1 Power/UTM NGX R65 with HFA 30, on an appliance-specific build (Take 46) of the Check Point SecurePlatform NGX R65 operating system.

A.3. Supported Nokia Firewall/VPN Appliances

The following Nokia models are included in the evaluated configuration for the security policy enforcement software (gateways), running the Nokia IPSO 4.2 build 051c05 operating system:

- IP150
- IP260
- IP290
- IP390
- IP560
- IP690
- IP1220
- IP1260
- IP1280
- IP2450