Security Gateway Appliances

R77

Security Target

Version 1.4

November 18, 2013

Prepared by:

Metatron Security Services

Metatron Security Services Ltd.

Check Point
SOFTWARE TECHNOLOGIES LTD.
We Secure the Internet.

Document Version Control Log

Version	Date	Author	Description
Version 0.1	July 13, 2009	Nir Naaman	Initial draft.
Version 0.5	December 7, 2009	Nir Naaman	Post-iVOR updates: removed FAU_SAA.4. Expanded description of L2TP support. Added FCS_CKM.1 and FCS_CKM.4 SFRs. Removed AVA_VAN.4 claim.
Version 0.9	September 7, 2011	Nir Naaman	Updated software version to R75, supporting IPSO and Gaia operating systems.
Version 1.0	December 31, 2012	Nir Naaman	Updated software version to R76. Removed support for IPSO. Incorporated virtualization functionality. Cryptographic enhancements: • Added support for SHA-256 integrity algorithm. • Key generation changed from X9.31 PRNG to SP 800-90 based hash DRBG (SHA-256). • SIC now uses 128 bit AES in place of Triple DES. • IPsec VPN supports both IKEv1 and IKEv2. • IKE now supports HMAC-SHA-256 and HMAC-SHA-384 keyed integrity algorithms. • IKE now supports Diffie-Hellman groups 19 and 20 (256 and 384-bit Random ECP). • IKE/IPsec now supports AES-GCM confidentiality and integrity algorithm. • Added support for ECDSA (P-256, P-384, and P-521). • Added support for TLSv1.1 and TLSv1.2 in SSL VPN and HTTPS Inspection. Added description of HTTPS Inspection functionality. Removed support for SecureClient Mobile. Clarified FRU_FLT.2 mappings.
Version 1.1	April 15, 2013	Nir Naaman	Updated references to R76 guidance documentation.

Version	Date	Author	Description
Version 1.2	September 18, 2013	SAIC	Updated to version R77, correcting product list, and dropping all claims regarding X9.31
Version 1.3	September 24, 2013	SAIC	Updated supported platform list.
Version 1.4	November 18, 2013	Leidos (formerly SAIC)	Added SecureXL reference.

Table of Contents

List of Tables

List of Figures

1. ST Introduction

1.1. ST Reference

Title: Security Gateway Appliances R77 Security Target

ST Version: 1.4

ST Date: November 18, 2013

Author: Nir Naaman

CC Version: Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 4, September 2012

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

Keywords: Information flow control, firewall, proxy server, traffic filter, remote access, VPN, SSL VPN, IPSec, IPS, intrusion detection

1.2. TOE Reference

TOE Software Identification: Check Point Security Gateway R77 in combination with Check Point Security Management R77, including the following software blades[1]:

- Security Gateway: Firewall, IPsec VPN, IPS, Acceleration and Clustering
- Security Management: Network Policy Management, Logging & Status, Monitoring

TOE software also includes a Management GUI product (SmartConsole R77) that is installed on a standard PC (outside the TOE) running a Microsoft Windows operating system.

TOE Hardware/Operating System Identification:

TOE Security Gateway appliances consist of the Gaia R77 operating system running Check Point Security Gateway software, on any of the hardware platforms listed in section 1.5.1.3 - TOE Hardware Platforms.

Check Point Security Management software is always installed on a separate platform running the Gaia R77 operating system, selected from the list given in Appendix A. The platform selected for this purpose is not used in the identification of the TOE.

TOE Support Program Identification:Enterprise Software Subscription[2].

[1] Software Blades are security modules purchased by customers independently or in pre-defined bundles, for installation on a Check Point Security Gateway or Security Management server.

[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.

1.3. Document Organization

Section 1 provides the introductory material for the security target, including ST and TOE references, TOE Overview, and TOE Description.

Section 2 identifies the Common Criteria conformance claims in this security target.

Section 3 describes the security problem solved by the TOE, in terms of the expected operational environment and the set of threats that are to be addressed by either the technical countermeasures implemented in the TOE or through additional environmental controls identified in the TOE documentation.

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

Section 5 is intended to be used to define any extended requirements claimed in this security target that are not defined in the Common Criteria.

Section 6 gives the functional and assurance requirements derived from the Common Criteria, Parts 2 and 3, respectively that must be satisfied by the TOE.

Section 7 explains how the TOE meets the security requirements defined in section 6, and how it protects itself against bypass, interference and logical tampering.

Section 8 provides supplemental information that is intended to aid the reader, including highlighting conventions, terminology, and external references used in this security target document

1.4. TOE Overview

1.4.1. Usage and Major Security Features of the TOE

Check Point Security Gateway Appliances are network perimeter security devices that provide controlled connectivity between two or more network environments.

Gateways may be installed as a standalone appliance, or as clusters of two or more appliances in a high-availability or load sharing configuration. Cluster members synchronize state tables, ensuring fault-tolerance with sub-second failover.

The product provides a broad set of information flow controls, including traffic filtering, application-level proxies, network address translation (NAT), and intrusion detection and prevention (IDS/IPS) capabilities. IKE/IPsec and SSL virtual private networking (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.

Information flow control functionality is implemented by one or more *Virtual Systems*. Each Virtual System is associated with two or more logical interfaces. Check Point Security Gateway Appliances maintain a separate domain of execution for each Virtual System, with separate security policies, state tables, configuration parameters, and audit logs. Routing tables are also virtualized, supporting the allocation of overlapping network address ranges for different Virtual Systems.

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

Check Point Security Gateway Appliances meet and exceed the requirements of three U.S. Government Protection Profiles, for proxy and traffic filtering firewalls and for IDS/IPS appliances

The evaluation assurance level claimed in this Security Target was augmented (in relationship to the assurance requirements specified in the claimed PPs) to EAL4 in order to provide additional assurance that the TOE is applicable to its target environments. A further augmentation for systematic flaw remediation (ALC_FLR.3) ensures that customers can register to receive the latest service packs and product versions.

1.4.2. TOE Type

Check Point Security Gateway Appliances are network perimeter security gateways. The product provides controlled connectivity between two or more network environments.

A network perimeter security gateway 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 gateway. This allows it to inspect, allow or deny and optionally modify these information flows.

Check Point Security Gateway Appliances can be installed and configured to be used as the product types listed in Table 1-1 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 1-1 specifies Check Point software blades that provide the relevant functionality.

Table 1-1 – Check Point Security Gateway Appliances Product Types

Product Type	Scope	Required Software Blade
Firewall and NAT gateway	☑	Firewall
IPsec VPN and Remote access / SSL[3] VPN gateway	☑	IPsec VPN
Intrusion detection and/or prevention	☑	IPS
Certificate management (PKI)	✓	Network Policy Management
Web Application Firewall (WAF)	✖	Web Security
VoIP Application Gateway	✖	Voice over IP (VoIP)
Router, Load balancer, and QoS enforcement gateway	✖	Advanced Networking
Security management product	✖	IPS Event Analysis, Reporting, Event Correlation, Provisioning
Cooperative enforcement (NAC)	✖	Endpoint Policy Management

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

[3] 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.

1.4.3. Non-TOE Hardware/Software/Firmware Required by the TOE

1.4.3.1. Management GUI Hardware and Operating System

The TOE includes three management GUI applications: 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 Security Management server.

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

- Windows 7
- Windows Vista (Ultimate, Enterprise, Business, Home Premium, or Home Basic) (SP1)
- Windows Server 2003 (Standard, Enterprise, or Datacenter Edition) (SP1-2)
- Windows Server 2008

Minimum hardware requirements for management GUI workstations are identified in the product release notes as follows:

- CPU – Intel Pentium IV or 2 GHz equivalent processor
- Memory – 512 Mb, Disk Space – 500 Mb
- CD-ROM drive, Video Adapter with minimum resolution: 1024 x 768

1.4.3.2. SSL VPN Client Hardware and Operating System

The TOE includes SSL Network Extender client-side software components (see section 1.5.1.7 below) 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. The software relies on the underlying hardware and operating system platform to provide cryptographic functions that support the TLS-based secure channel established with the TOE, and to route applicable traffic through this channel.

The SSL Network Extender client can be distributed (i.e. downloaded from the TOE) as an Active X control, a trusted Java applet, or as a MSI object. Its functionality is equivalent in all of these cases. The client-side user interface is based on a standard Web browser, displaying HTML pages provided by the TOE.

The following operating environments (or later versions thereof) are supported:

- SSL Network Extender
    - Windows 2000 Professional
    - Windows XP Home Edition or Professional

  - Windows Vista

- The following browsers are supported for activating SSL Network Extender:
  - Microsoft Internet Explorer version 5.0 or higher
  - FireFox
  - Safari
- The following Java Virtual Machine (JVM) versions are supported for the SSL Network Extender Java applet:
  - JVM 1.1 and higher

1.5. TOE Description

Check Point Security Gateway Appliances provide 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[4].

The TOE Description consists of the following subsections:

- **Physical Scope of the TOE** – describes the hardware, firmware, and software parts that constitute the TOE and their relationship with the product.
- **TOE Guidance** – identifies the guidance documentation that is considered to be part of the TOE.
- **Logical Scope of the TOE** – describes the claimed logical security features offered by the TOE and the product features excluded from the evaluated configuration.
- **Check Point Services** – describes vendor services that complement the TOE, providing systematic flaw remediation, software updates, and IDS/IPS updates.

[4] 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.

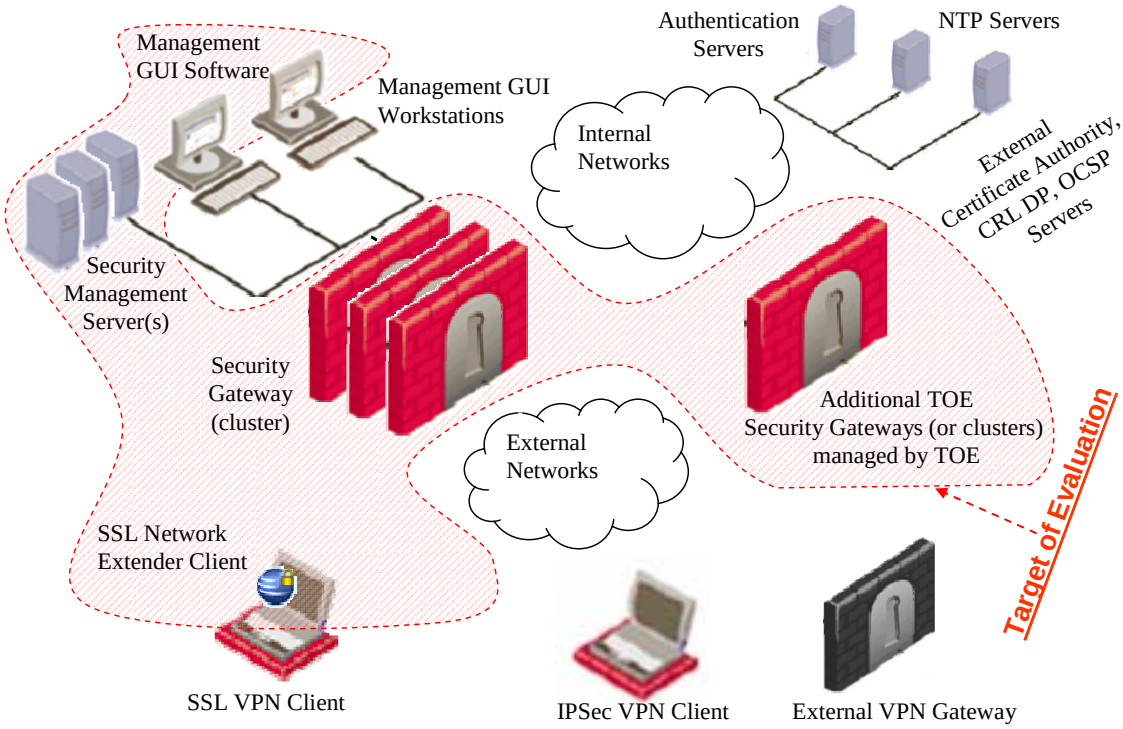
1.5.1. Physical Scope of the TOE

1.5.1.1. Definition

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

- Check Point Security Gateway Appliances, including Security Gateway software, Gaia operating system, and appliance hardware; and
- Security Management servers, including Security Management software, Gaia R77 OS, and hardware platform; and
- SmartConsole Management GUI software; and
- SSL Network Extender (SSL VPN) client software; and
- TOE guidance.

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



1.5.1.2. TOE Interactions with its Operational Environment

The TOE enforces network traffic information flow policies on traffic flowing through Check Point Security Gateway Appliances. The TOE relies on the IT environment to route all controlled network traffic flows through the appliances.

The TOE does **not** include the following components that may interact with the TOE:

- Management GUI hardware and operating system (see section 1.4.3.1 above).

- Networking equipment (routers, bridges, switches, etc.) that is used to connect between distributed TOE components as well as connect the TOE to internal and external networks.
- The TOE may be configured to interact with external servers:
  - External authentication server implementing single-use authentication using the RADIUS or SecurID protocols.
  - External Certificate Authority (CA).
  - External certificate validation server (HTTP or LDAP CRLDP, OCSP).
  - External NTP time-synchronization server.
- External (non-TOE) VPN gateways for the establishment of secure VPN channels using the IKE/IPsec protocols.
- SSL VPN client hardware and operating system (see section 1.4.3.2 above).
- IPsec VPN clients[5].

1.5.1.3. 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, A.3 and A.4.

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.

1.5.1.4. TOE Security Gateway Software

Check Point Security Gateway R77 Security Gateway software 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 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. Check Point has developed a proprietary kernel-level infrastructure that provides an execution environment for kernel processing, including memory management, communication, and scheduling facilities. CoreXL technology allocates firewall, IPS, and VPN processing tasks to available CPU resources, leveraging generally-available commercial multi-core processors with near-

[5] Note: Although the CD-ROM package described below includes Check Point IPsec VPN client applications (Check Point Endpoint Connect and Check Point SecureClient), these software applications are not considered part of the TOE and are licensed separately. See section 1.5.1.8 for a partial list of supported clients.

linear scalability. SecureXL is a framework that accelerates Security Gateway performance.

Alternatively, when multiple virtual systems are defined on a gateway, TOE security functionality is moved to operating system user space, with separate processes allocated for the different virtual systems.

The Security Gateway software, OS and hardware platform are all collectively identified in this ST as 'Check Point Security Gateway Appliances'. Check Point Security Gateway Appliances are delivered to the customer with all software pre-installed, and a backup copy of the installed software is provided on a CD for backup and reference purposes.

1.5.1.5. TOE Management Architecture

The Check Point Security Gateway Appliances' CD-ROMs also contain Security Management software, SmartConsole Management GUI software, and a Check Point proprietary OS identified as Gaia R77, a stripped-down version of the Linux operating system.

Security Management software is installed in conjunction with the operating system on hardware platforms selected from the list of supported platforms in Appendix A. The Security Management software, OS and hardware platform are collectively identified in this ST as the 'Security Management server'.

One or more Security Gateway appliances are managed by a Security Management server installation that maintains security policy information for the gateways, and collects audit records from the gateways for review by TOE administrators.

Multiple Security Management servers synchronize security policy and user databases using Management High Availability functionality, so that if the active server fails, an authorized administrator can manually transition a standby server to the active mode. Security Gateway appliances can be configured to send audit and IDS System log records to multiple Security Management servers to ensure that log data is accessible on both active and standby Security Management servers.

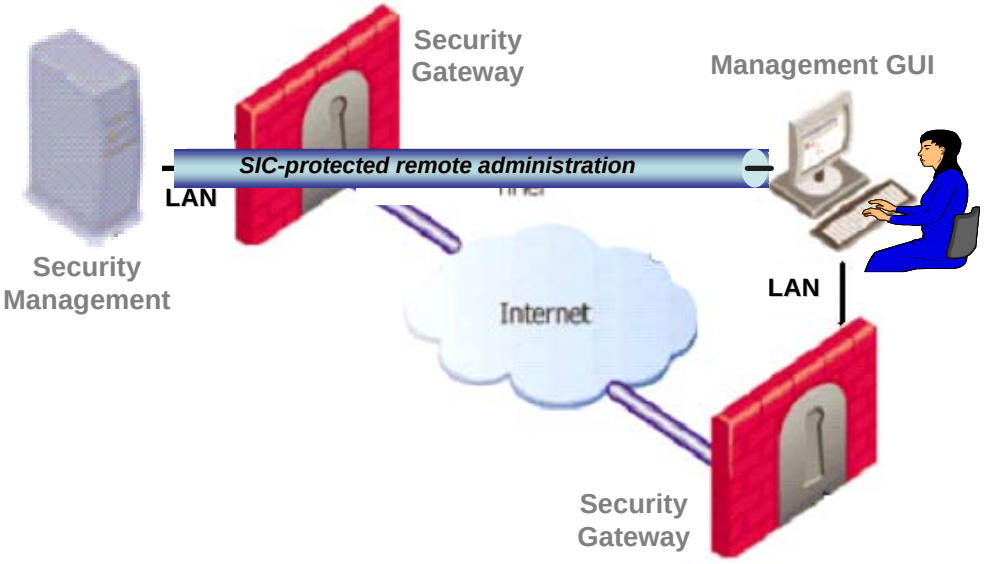
As described in the TOE evaluated configuration guidance, Security Management servers must be installed on a protected subnet that is directly connected to a TOE Security Gateway appliance. The appliance protects the Security Management server from any direct network access by untrusted entities. The Security Management server may manage this gateway appliance, as well as other remote Check Point Security Gateway Appliances. Administrators connect to the Security Management server installation using management GUI software running on administrator workstations.

The evaluated configuration supports both local and remote administration:

- *Local administration*: a management GUI is directly connected to the Security Management server Local Area Network (LAN) (as in Figure 1-1 above); or
- *Remote administration*: a management GUI is installed on a protected LAN that is directly connected to a remote TOE Security Gateway appliance.

Note: the term 'local administration' is used in this ST as defined above, and is not meant to imply the use of a directly-connected console device.

Figure 1-2 - Remote administration of the TOE



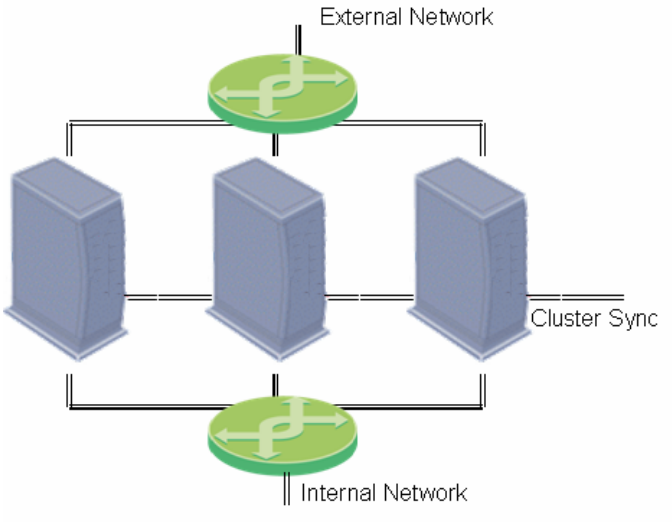
In both local and remote administration configurations, TOE evaluated configuration guidance requires the administrator workstation to be deployed on a protected subnet that is directly connected to a TOE Security Gateway appliance. The appliance protects the workstation from any network access by untrusted entities. The workstation operating system and hardware do not contribute any security functionality, and are considered to be outside the boundaries of the TOE.

Note: all TOE internal management communications are protected using the Secure Internal Communications (SIC) security function, which is based on the TLSv1.0 protocol using the FIPS-approved AES encryption algorithm. This includes all communications between management GUIs and Security Management server hosts, communications between multiple Security Management server hosts, and communications between Security Management server hosts and managed gateways.

1.5.1.6. Security Gateway Cluster Configurations

In cluster configuration, the Security Gateway is in fact two or more Check Point Security Gateway Appliances installed in parallel. A cluster provides identical functionality to a single gateway, but can provide enhanced performance and fault tolerance. Cluster members are all attached identically to internal and external networks; in addition, each member is attached to one or more dedicated cluster synchronization networks that are isolated by the gateways from any external access. Cluster members synchronize their state tables using Check Point ClusterXL technology, supporting automatic failover and load balancing between cluster members.

Figure 1-3 –Security Gateway Cluster Configuration



1.5.1.7. SSL VPN Clients

The TOE includes SSL Network Extender 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.

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 1-4 - SSL Network Extender running in standard Web browser

Users can download and install the SSL Network Extender client software directly from a Check Point Security Gateway Appliances, 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.

1.5.1.8. 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 Endpoint Security, and Check Point Endpoint Connect. Some third party IPsec VPN clients have also demonstrated interoperability with the TOE. In addition, the TOE supports native IPsec L2TP clients included in various operating systems, such as Microsoft Windows operating systems and Apple iPhones.

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

1.5.2. TOE Guidance

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

Title	Date
R77 CC Evaluated Configuration Installation Guide	April 2013
R77 CC Evaluated Configuration Administration Guide	April 2013
R77 Gaia Administration Guide	26 August 2013
Security Management Server R76 Administration Guide	21 January 2013
Security Gateway R77 Technical Administration Guide	29 August 2013
SmartView Monitor R77 Administration Guide	20 August 2013
SmartView Tracker R77 Administration Guide	19 August 2013
Check Point IPS R77 Administration Guide	26 August 2013
Firewall R77 Administration Guide	27 August 2013
VPN R77 Administration Guide	20 August 2013
ClusterXL R77 Administration Guide	26 August 2013
Check Point VSX R77 Administration Guide	26 August 2013
VPN-1 FIPS 140-2 Non-Proprietary Security Policy	

1.5.3. Logical Scope of the TOE

1.5.3.1. Summary of TOE Security Functionality

Check Point Security Gateway Appliances 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 authentication credentials held by the user. Administrators also need to authenticate to the TOE before they can use the Management GUIs to access Security Management. The TOE can be optionally configured to perform user authentication with the support of external authentication servers in the IT environment.

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.

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.

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. The TOE can be configured to perform IDS analysis on encrypted HTTPS streams, by terminating the HTTPS connection from the client on the gateway, applying HTTPS Inspection, and establishing a corresponding HTTPS connection to the server.

Administrators can perform both local and remote management of the TOE. Administrator sessions are protected via a trusted path between the Management GUI and the Security Management server. Internal TOE communications between the Security Management server and Security Gateway appliances is also protected from disclosure and undetected modification.

Audit trail and IDS System data is stored in log databases, 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 log storage is exhausted, then the only recordable 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 and IDS System data according to attributes of the data recorded and ranges of some of those attributes.

The Check Point Security Gateway Appliances Security Gateway appliance protects itself and the Security Management server and Management GUIs against network-level attacks by unauthorized users. 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.

Fault-tolerance is ensured by supporting multiple Security Gateway appliances and Security Management hosts that synchronize databases and state tables among redundant instances. Critical hardware, software, and networking components are constantly monitored, allowing the TOE to reconfigure itself to bypass faulty components.

1.5.3.2. 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 Security Gateway Appliances product supports a separately-licensed IPv6 dual-stack capability; however, this support is not enabled by default, and is not enabled in the evaluated configuration.

Routed packets are forwarded to a TOE interface with the interface's MAC address as the layer-2 destination address. The TOE routes the packets using the presumed destination address in the IP header, in accordance with route tables maintained by the TOE.

IP packets are processed by the Check Point Security Gateway Appliances software, 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.

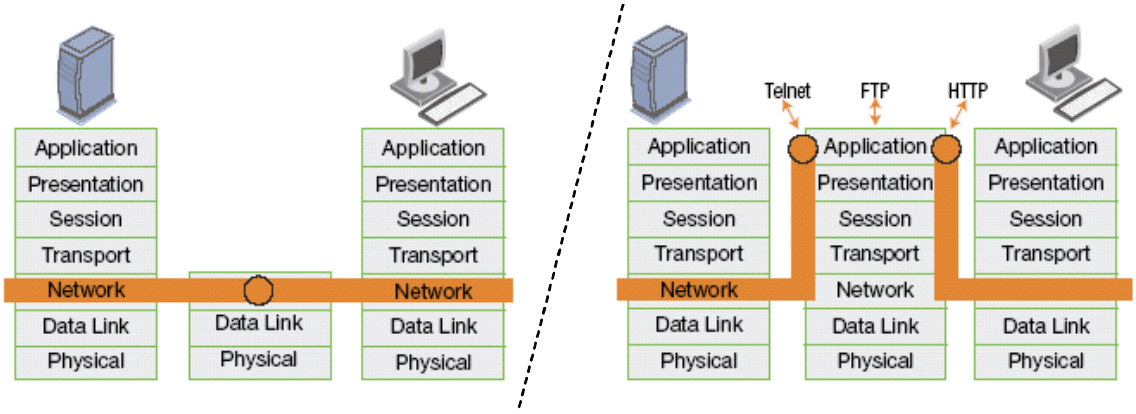
Network Address Translation (NAT) rules can modify source and/or destination addresses and/or UDP or TCP ports according to administrator-defined policies, supporting configurations where communicating end points do not interact with the actual IP address of their peers.

1.5.3.3. 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 1-5- Traffic filtering (left) vs. Application-level Proxies



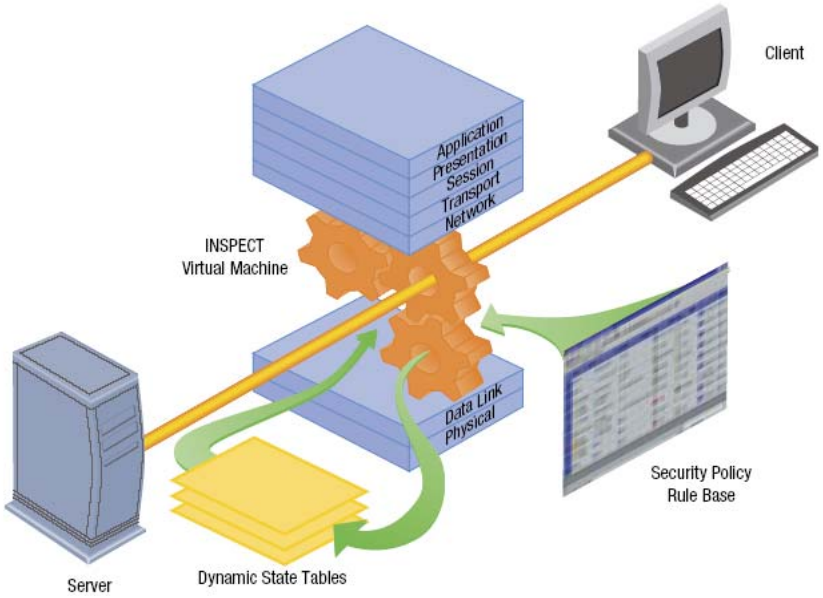
Check Point Security Gateway Appliances provides both traffic-filtering capabilities and application-level proxies. In addition, the product provides a capability for Stateful Inspection. With Stateful Inspection, packets are intercepted at the network layer (as in a traffic filter), but the firewall 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 packets 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[6] 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 Check Point Security Gateway Appliances as a kernel-level virtual machine. Security policy is compiled on the Security Management 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 1-6 - Stateful Inspection



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 1-7- Example Rule

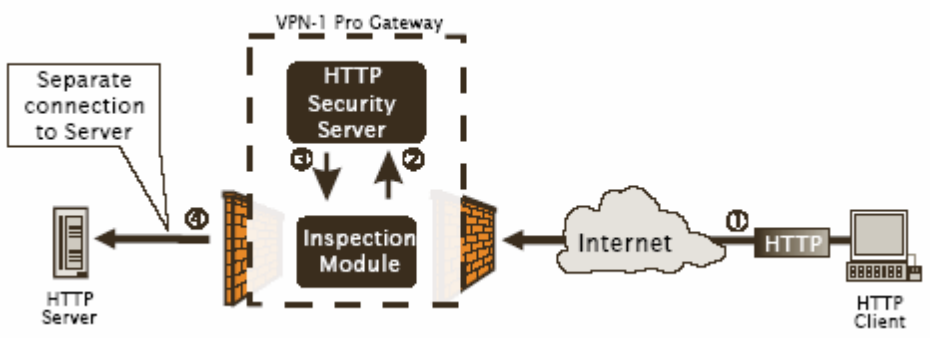
SOURCE	DESTINATION	VPN	SERVICE	ACTION	TRACK	INSTALL ON	TIME
Alaska LAN	* Any	* Any Traffic	TCP http	accept	Log	* Policy Targets	* Any

[6] U.S. Patent 5,606,668, *System for securing inbound and outbound data packet flow in a computer network.*

1.5.3.4. 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 1-8- Security Servers



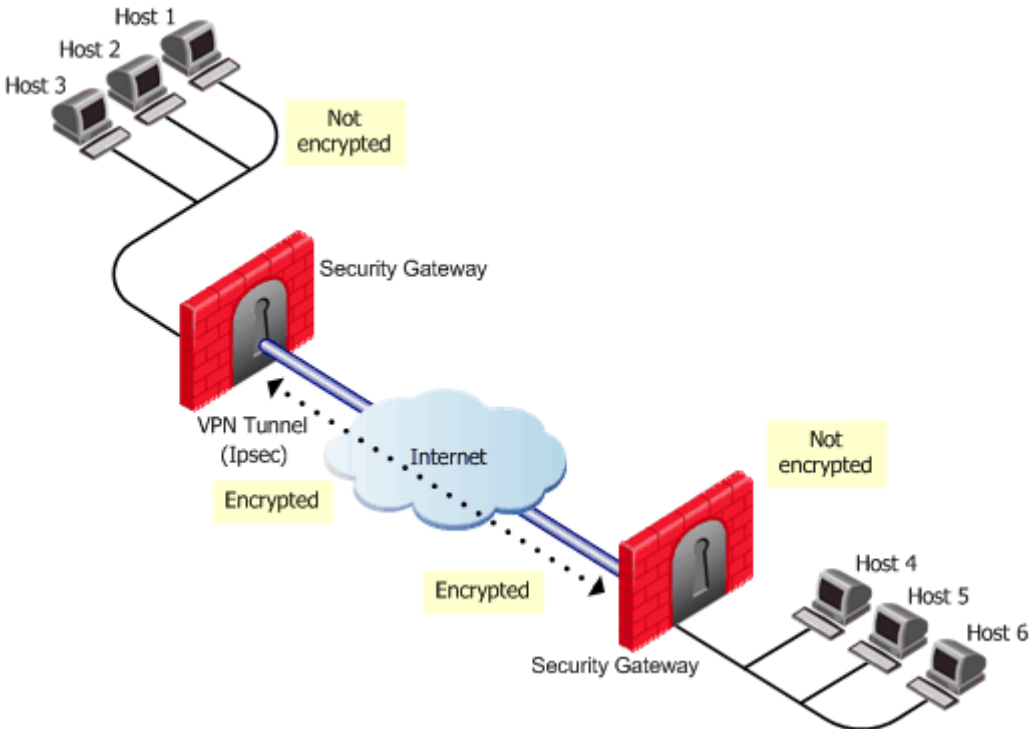
For proxied information flows, the TOE may be configured by an authorized administrator to send the information to a server in the IT environment using a Check Point proprietary Content Vectoring Protocol (CVP) or URL Filtering Protocol (UFP). This is typically used for integration with anti-virus or 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.

1.5.3.5. 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 1-9- Virtual Private Network



A TOE Security Gateway can be configured 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 or mobile device (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.

Gateways authenticate themselves to their VPN peers using public key certificates or IKE shared-secret authentication. The product supports a number of remote access VPN user authentication mechanisms, including certificate-based authentication, multiple-use passwords, as well as authentication using an external server in the IT environment – using the RADIUS, SecurID, LDAP, TACACS, or TACACS+ protocols[7].

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.

[7] In the TOE evaluated configuration, only RADIUS and SecurID are supported for communication with an external authentication server in the IT environment. If an external SecurID authentication server is used, it must be installed on a protected subnet that cannot be accessed by untrusted users. Only single-use authentication mechanisms are allowed in the evaluated configuration, whether authenticated exclusively by the TOE or with the support of the IT environment.

The TOE performs certificate revocation checks using the protocols LDAP or HTTP, and also supports the OCSP protocol for performing online revocation checks.

Both IPsec and SSL VPN capabilities support NAT traversal, so that VPN tunnels can be created even when address translation is applied on network traffic between VPN peers.

1.5.3.6. 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.

A VPN community is defined as a collection of VPN gateways. Topology definitions created by an 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.

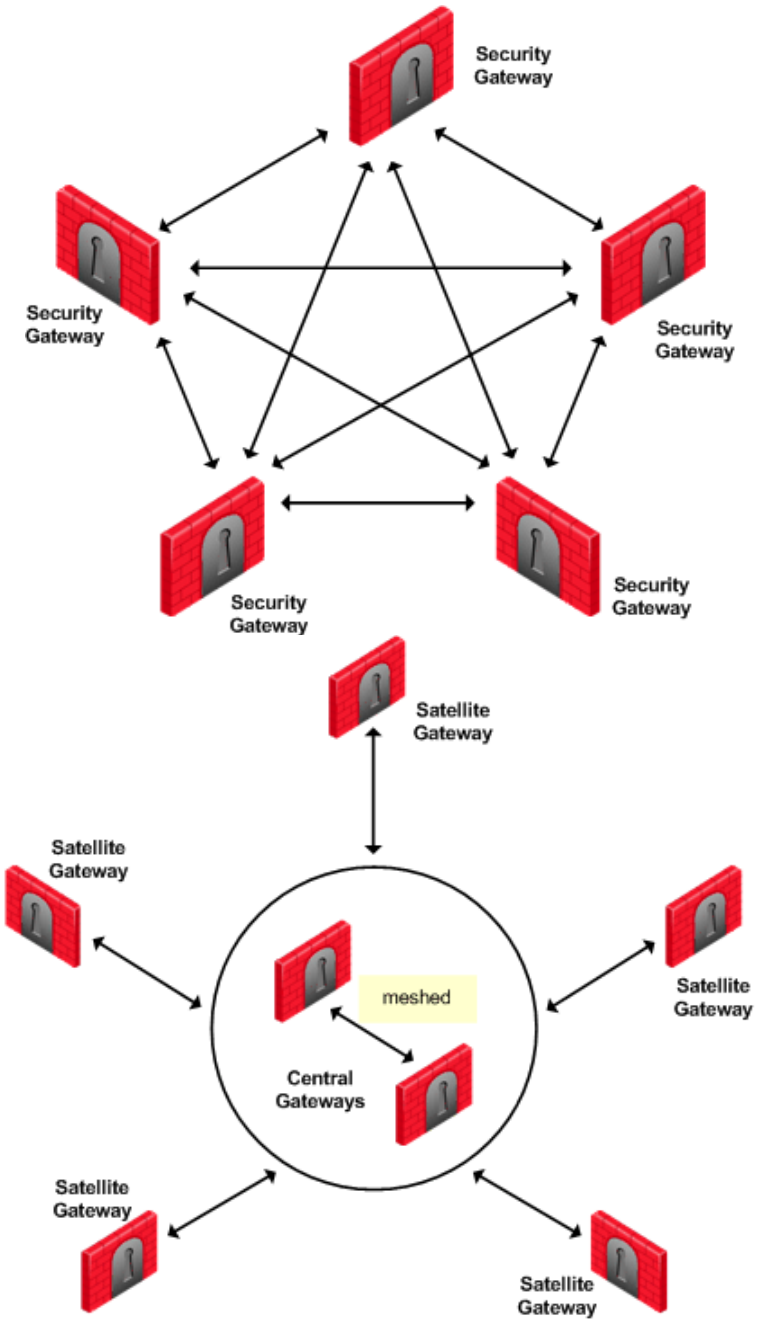
Conversely, tunneled traffic received by the gateway from a VPN peer is decrypted and verified using the corresponding VPN community security attributes, before being forwarded to its presumed destination address.

VPN community topology may be *Meshed*, where any traffic between VPN domains of the community's gateways is tunneled, *Star*, 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). Complex VPN architectures can be defined without having to resort to manually defining each VPN tunnel created between any two gateways.

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

Figure 1-10- Examples of Meshed and Star VPN Communities



VPN community settings are orthogonal[8] 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.

[8] In *Wire Mode*, an authorized administrator may configure a gateway to exempt specific verified VPN traffic flows from traffic filtering. For example, for a given Star community configuration, the central gateways may be configured to allow through verified VPN traffic flowing between two satellite gateways without further filtering, while applying the traffic filtering rule base on each of the satellite gateways.

In the example given in Figure 1-11 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 1-11- VPN community used as a Rule Base security attribute

1.5.3.7. Extended VPN Capabilities

Check Point Security Gateway Appliances support extended VPN modes that solve connectivity issues with remote access clients. These modes include:

Visitor mode – The TOE supports a mode intended for remote access clients that are restricted to Web access. With Visitor mode, IKE, IPsec, and TLS traffic is tunneled through a single TCP port, 443 by default.

Office mode – the TOE allocates an internal IP address to the remote access client, which is then used as the client source address inside the VPN tunnel. Office mode involves an extension to the IKE protocol exchange.

Hybrid mode - IKE Phase I supports either certificate-based or shared secret-based authentication. Check Point Security Gateway Appliances supports a hybrid mode for remote access clients where the gateway authenticates using a certificate, and the client authenticates using a password that can be authenticated with the help of an authentication server in the IT environment.

Multiple Entry Points (MEP) - Check Point Security Gateway Appliances respond to unauthenticated connectivity queries over a proprietary Check Point RDP[9] protocol. This allows remote access VPN clients and VPN gateways to select a peer gateway in configurations where a target VPN domain has multiple entry points.

IPsec/L2TP– the TOE supports standard IPsec/L2TP implementations provided natively in some desktop and mobile platform operating systems. After an IKE/IPsec channel is established by the remote access VPN client, authenticating the client platform identity, an additional L2TP exchange is performed within the trusted channel, authenticating the user. Supported user authentication mechanisms include certificate-based authentication (using EAP-TLS), EAP/CHAP MD5-challenge multiple-use password-based authenticators (not allowed in the TOE evaluated configuration), and PAP passwords authenticated with the help of an authentication server in the IT environment.

[9] 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.

1.5.3.8. Intrusion Prevention System (IPS)

Check Point Security Gateway Appliances provides a multi-layer IPS engine that is integrated into the Security Gateway kernel. Traffic that has been allowed by the firewall and VPN security policies is matched against a combined set of protocol enforcement and pattern matching logic that identifies suspicious network traffic and assigns Confidence Level (that the traffic indeed contains an attack) and Severity (potential impact of the attack on protected resources) security attributes to the traffic. Based on these attributes and on administrator-specified security policy settings, the IPS engine may take action by generating applicable log records (Detect) and optionally blocking the traffic (Prevent).

IPS engine logic consists of the following layers:

- **Passive Streaming Library (PSL)** – an in-kernel TCP stack that assembles IP packets into information streams for IPS protocol parsers.
- **Protocol Parsers** – implement protocol-specific state machines that enforce protocol compliance and detect protocol anomalies that may be indicative of an intrusion attempt. The protocol parsers extract protocol 'contexts' from the information streams. A context is a well defined part of the protocol, on which further security analysis can be performed, e.g. a HTTP URL, HTTP headers, HTTP response, etc. The HyperSPECT feature provides performance optimization for the processing of rules involving the body of HTTP packets.
- **Context Management Interface** – coordinates application of protections defined in the security policy on contexts established by protocol parsers.
- **Pattern Matcher** – a two-tier pattern matching engine that matches information streams against IPS attack signatures. The first tier applies simple matching criteria that separate clearly harmless traffic from the rest. Traffic not matched by the first tier is inspected by the second tier, which performs deeper inspection through the use of regular expression matching or execution of INSPECTv2[10] signature matching programs for identifying suspicious activity.
- **Compound Signature Identification** – matches complex signatures that are triggered when a defined logical condition over multiple contexts is matched. The logical expression can use AND, OR, NOT or ORDERED-AND to construct the logical expression. An example of CSI use is a CAPICOM protection which looks for one of three signatures. If one is found, then it looks for another signature to validate the finding. Only when all patterns are matched are the protections triggered and the appropriate action taken.

IPS logic updates may be downloaded from a Check Point IPS Update subscription service over a secure channel established to a Check Point Web site, or imported manually into the TOE by an administrator. Updates are installed as regular expressions and INSPECTv2 code fragments, and are packaged with corresponding GUI updates to

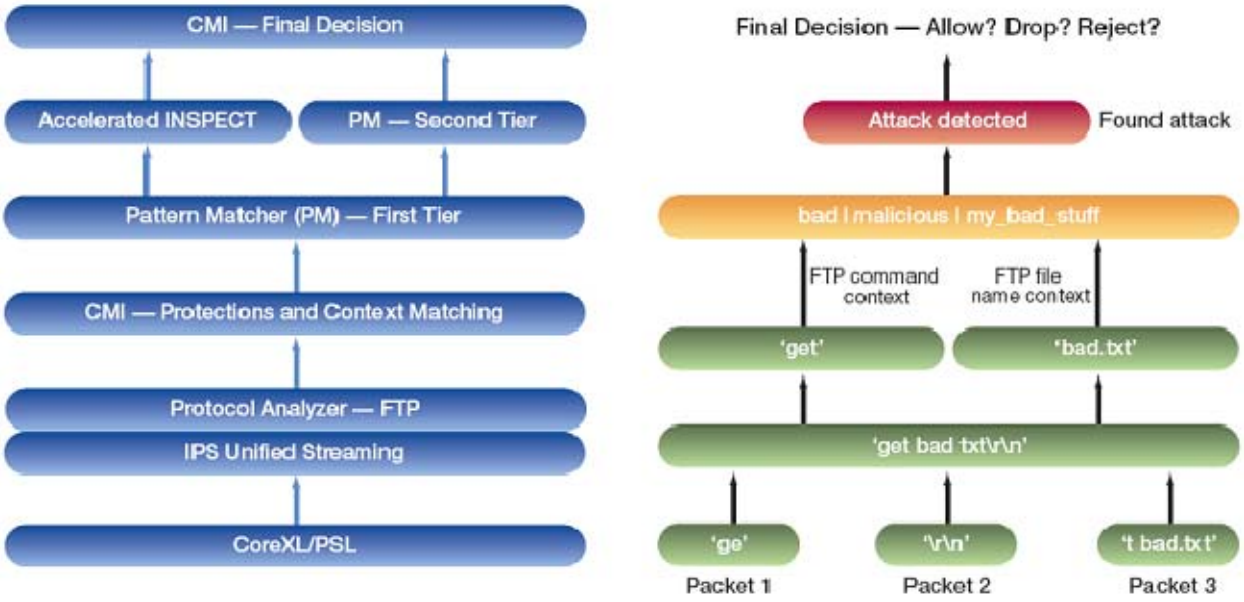
[10] INSPECTv2 is an extension of the Check Point INSPECT language used by the TOE for Stateful Inspection, leveraging concepts from the N-Code language used in the Check Point IPS-1 product.

integrate seamlessly with previously installed defenses, while maintaining the TOE within its evaluated configuration.

Figure 1-12 depicts an example IPS signature match for the FTP protocol. The left side of the figure depicts the IPS engine logic layers described above. The right side shows the incoming IP packets (on the bottom right of the figure) and the processing performed by the different logic layers, depicted from the bottom of the figure upwards.

In the example, the attacker attempts to access an unauthorized file ('bad.txt') using a FTP 'get' command. The attacker attempts to obfuscate the attack by fragmenting the command over three IP packets, reordering them so that the 'get' command must be reconstructed from the first and third packets. The PSL layer (bottom left) converts the IP packets received by the Security Gateway into protocol streams that are examined by the FTP protocol analyzer, extracting two contexts: command and file name. The Pattern Matcher matches a known attack signature, and signals a detected attack, allowing the Security Gateway to take appropriate action (Allow, Drop, or Reject).

Figure 1-12 - Example IPS Signature Match



1.5.3.9. HTTPS Inspection

IPS analysis and reaction can be applied on encrypted HTTPS streams. HTTPS inspection is configured as an ordered set of rules that define which network traffic streams will be inspected and which streams will be allowed through the TOE without further IPS inspection. For example, the rule base depicted in Figure 1-13 below requires inspection and logging of all outbound HTTPS traffic excluding users that belong to the CEO_office, and excluding traffic outbound to Web sites that have been categorized as email, financial services or health related.

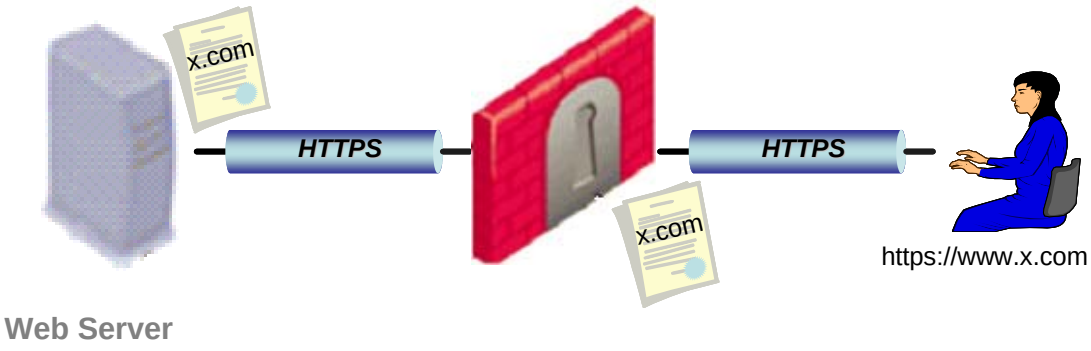
Figure 1-13 - Example HTTPS Inspection Rule Base

No.	Name	Source	Destination	Services	Site Category	Action	Track	Blade
1		CEO_office	Internet	TCP https TCP HTTP_and_H...	Any	Bypass	None	All
2		Any	Internet	TCP https TCP HTTP_and_H...	Email Financial Services Health	Bypass	None	All
3		Any	Internet	TCP https TCP HTTP_and_H...	Any	Inspect	Log	All

HTTPS Inspection is applied as follows. When an HTTPS connection request matches an Inspect rule in the rule base, the Security Gateway attempts to establish a corresponding HTTPS connection from the gateway to the requested Web server. If the server's certificate can be validated successfully, the gateway completes the TLS session establishment with the client, using a certificate that identifies the requested Web server, but is stored on the gateway. This certificate can be configured to be a "real" Web server certificate that is pre-loaded onto the gateway, or a "fake" that is generated and signed on-the-fly by the gateway.

Once both client-to-gateway and gateway-to-server HTTPS connections have been established, the gateway proxies information between client and server, applying the configured IPS protections on the plaintext information traffic.

Figure 1-14 - HTTPS Inspection



1.5.3.10. User Authentication

The TOE can be configured 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), multiple-use passwords stored on Check Point Security Gateway Appliances, as well as authentication using an external server in the IT environment – using RADIUS, SecurID, LDAP, TACACS, or TACACS+ protocols[11].

[11] In the TOE evaluated configuration, only RADIUS and SecurID are supported for communication with an external authentication server in the IT environment. If an external SecurID authentication server is used, it must be

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. Multiple-use passwords should not be configured in the evaluated configuration. If an external SecurID authentication server is used, it must be installed on a protected subnet that cannot be accessed by untrusted users.

Administrators are authenticated using certificates that are issued by the Internal Certificate Authority (see below), or via RADIUS or SecurID authentication.

1.5.3.11. Virtual Systems

The TOE provides an abstraction of *Virtual Systems* (VSs) and virtual networking entities (virtual routers and switches). Virtual Systems are associated with physical and logical (VLAN-tagged) interfaces. The TOE maintains separate execution domains for each Virtual System, including configuration, state tables, routing (VRF) tables, ARP tables, logging information, and security policies.

Virtual Systems provide virtually equivalent functionality to the corresponding use of multiple physical gateways deployed in each networking domain or enclave. The TOE allows information to flow between Virtual Systems or between interfaces associated with different Virtual Systems only if an administrator explicitly connects these Virtual Systems using virtual networking entities.

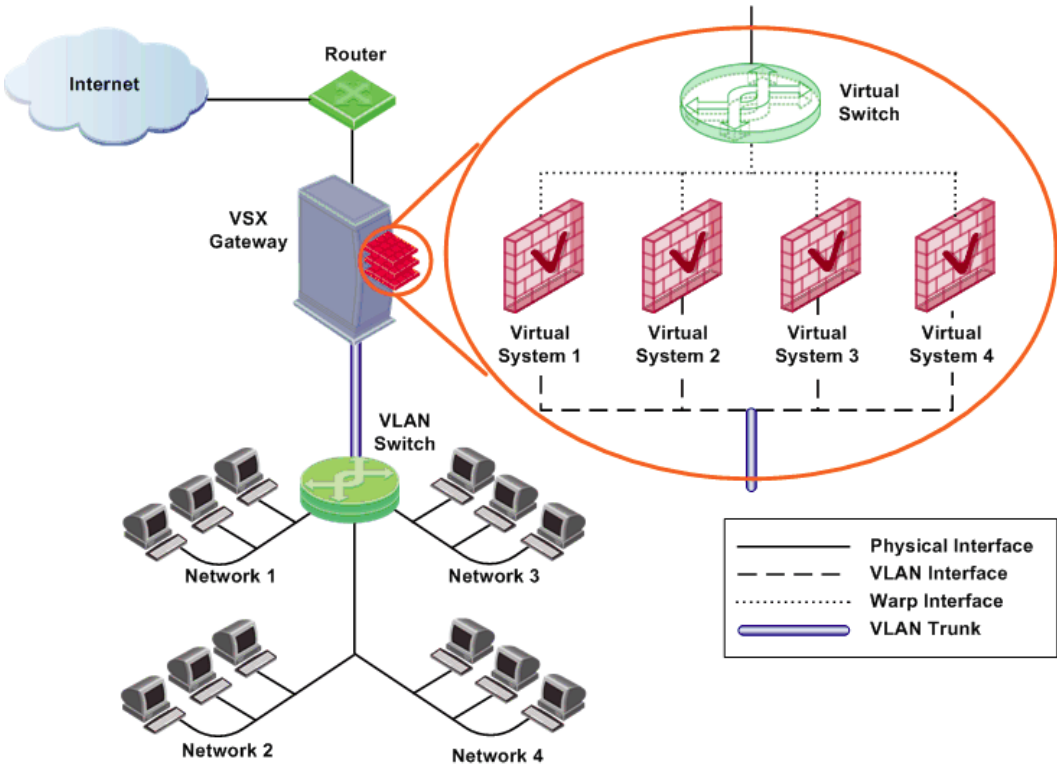
Check Point's INSPECT virtual machine engine supports the definition of separate execution domains for Virtual Systems. Incoming IP packets bind to an appropriate VS corresponding to the logical interface (i.e. physical or virtual LAN interface) on which they are received, and the VS that is defined to receive the packet from that interface. The packets are labeled with the VSID, and are handled in the context of that VS's execution domain, until they are dropped, forwarded out of the gateway, or handed to another VS according to administrator-defined rules.

The Virtual System abstraction allows the administrator to model virtually any multi-gateway networking configuration. Supported Virtual System types include:

- **Virtual System** – a fully-functional firewall, NAT, IDS/IPS, VPN gateway.
- **Virtual Router** – routes IP packets between VSs and TOE interfaces, does not filter traffic.
- **Virtual Switch** – provides layer-2 connectivity between VSs and TOE interfaces, does not filter traffic.

installed on a protected subnet that cannot be accessed by untrusted users. Only single-use authentication mechanisms are allowed in the evaluated configuration, whether authenticated exclusively by the TOE or with the support of the IT environment.

Figure 1-15 - Virtualization – a Typical Configuration



1.5.3.12. TOE Management

As described in section 1.5.1.5 above, the TOE provides a highly-scalable, fault-tolerant three-tier management architecture that supports both local and remote management. All TSF data is maintained on the Security Management installation, and accessed by administrators using management GUIs. Security Management distributes network configuration and security policy information to Security Gateways, and collects audit records for storage and review.

Management interfaces consist of the SmartConsole Management GUI applications, including SmartDashboard, SmartView Tracker, and SmartView Monitor. These interfaces allow an 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.

The TOE associates administrator accounts with granular permissions, providing control of the functions that the administrator may access. In this ST, three security management roles are defined: the authorized administrator role is a human user that may perform all security management operations; the authorized audit administrator is authorized to review audit trail and IDS System data; and the OPSEC client is authorized to use the OPSEC APIs described in section 1.5.3.14 for audit trail and System data review and for adding IDS System data.

The TOE can be configured to generate alerts for selected events. Alerts can be displayed in a pop-up window on the SmartView Monitor management GUI application, or can be sent to an external IT entity as an SNMP trap or email.

1.5.3.13. Internal/External Certificate Authority (ICA)

The Security Management 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 Security Management server and managed Check Point Security Gateway Appliances. The ICA publishes CRLs internally to TOE components. The ICA also generates administrator certificates.

All internal communications between the Management GUI and the Security Management server, between the Security Management server and Check Point Security Gateway 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).

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

1.5.3.14. OPSEC Client APIs

Security Management server provides a set of APIs (and corresponding network protocols) for Check Point OPSEC partners that support integration of third-party management products.

The TOE evaluated configuration supports the following interfaces:

- **LEA** (Log Export API) – allows external authorized IT entities to receive audit records collected by the TOE.
- **ELA** (Event Logging API) – allows external authorized IT entities to send log records to the TOE to support centralized event management using SmartView Tracker and other Check Point management products.
- **AMON** (Application Monitoring) – allows third party products to provide application status monitoring information that can be displayed in the SmartView Monitor management GUI.

OPSEC API clients authenticate to the TOE using SIC certificates, and are bound by the permissions and restrictions associated with the corresponding OPSEC protocol.

1.5.3.15. Fault Tolerance

Fault tolerance is ensured through redundancy. Multiple Security Management server hosts and Security Gateway appliance ensure that when a failure is detected on an active host or gateway, the TOE can transfer control to a standby host or gateway.

As described in section 1.5.1.5 above, configuration of multiple Security Management server hosts allows the administrator to manually transition to a standby server if the active server fails.

Section 1.5.1.6 describes ClusterXL Security Gateway clustering configurations. Security policy is installed on all cluster members, and state information is synchronized over dedicated synchronization network interfaces, allowing the TOE to transfer information flow control processing between cluster members without connection loss[12].

Check Point Security Gateway Appliances support multiple clustering modes, including:

- **High Availability Mode**– in this mode, one cluster member is active, while the other members are in the standby state. The active member distributes state table information to the standby members. If a failure is detected on the active member, the highest priority standby member transitions to the active mode, and continues to process network information flows in place of the failed member.
- **Load Sharing Mode** – in this mode, information flow processing is performed by all cluster members concurrently, distributing processing load across all available CPU resources. If a failure is detected on a cluster member, network traffic is redistributed among the operational members.
- **Virtual Router Redundancy Protocol (VRRP)** – cluster members use industry standard election protocols to elect one cluster member as the active member that processes information flows through the TOE. If the active member fails, another cluster member is transitioned to the active state.
- **VSX Gateway High Availability** – in this mode, virtual entities are duplicated on multiple cluster members. If a cluster member fails, its virtual entities are executed by another member. In configurations where Virtual Systems are independent (i.e. are not connected using Virtual Routers or Virtual Switches), failover can also be performed on an individual Virtual System level.
- **Virtual System Load Sharing (VSLS)** – in this mode, the cluster automatically distributes Virtual Systems among all operational cluster members, in accordance with administrator-defined Virtual System priorities and weights. Each Virtual System in the Active state synchronizes its state tables with a Standby on another cluster member. When a cluster member fails, the Standby Virtual Systems become Active.

[12] Some types of connections do not survive cluster failover, because they are associated with state information that cannot be replicated. In particular, proxied connections are not replicated, because they are processed by security servers that run outside the Security Gateway kernel. In addition, certain types of IPS streaming applications use non-replicated state; an administrator can specify whether they should be closed on failover (fail-safe) or survive it even at the risk of false-negative verdicts on these connections (fail-open).

1.5.3.16. Time Synchronization

Check Point Security Gateway 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), Check Point Security Gateway Appliances 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 Security Management 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 Security Management server, and can be reviewed individually.

1.5.3.17. Functionality Excluded from the TOE Evaluated Configuration

Table 1-1 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:

- **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 Security Gateway Appliances
  - The attachment of product licenses to Check Point Security Gateway Appliances

  SmartUpdate is implemented via a Remote Installation daemon that is disabled when the TOE is in FIPS mode.
- **SNMP daemon** – Check Point Security Gateway Appliances provide SNMP support for remote management by third-party monitoring systems. This includes an SNMP agent for SNMP v1, v2c, and v3 (USM) protocol versions, as well as a variety of MIBs allowing intuitive and standards-based support for monitoring device utilization, High Availability, interoperation of devices and Check Point VPN-1 utilization as well as traffic load monitoring. SNMP support is disabled when the TOE is in FIPS mode.
- **Dynamic Routing** - Check Point Security Gateway Appliances can be configured to support dynamic routing protocols that are used to exchange network topology information with other bridges and routers. Supported protocols include the OSPF, RIP, and BGP unicast dynamic routing protocols and the IGMP, PIM-SM, and PIM-DM multicast dynamic routing protocols. Configuration of dynamic routing is supported only via a CLI, and is thus not available in the evaluated configuration.
- **WebUI** – Gaia provides a Web-based configuration interface as an alternative to the Check Point Security Gateway Appliances appliance CLI. This interface is not available when the TOE is in FIPS mode.
- **CLIs and SSH** - Check Point Security Gateway 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 Security Management server. The CLI can be accessed from a directly connected console or remotely using the SSH protocol[13].

[13] SSH access is disabled when the Check Point Security Gateway Appliances are in FIPS mode.

In the evaluated configuration, these CLIs should not be used after this installation stage. All management of the TOE should be performed via the Security Management 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.

1.5.4. Check Point Services

1.5.4.1. 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.

1.5.4.2. 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 sk97764 provides resources related to this evaluation including TOE guidance and utilities for setting up the evaluated configuration. It is available for General Access.

1.5.4.3. 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.

1.5.4.4. Enterprise Software Subscription

TOE users must purchase an Enterprise Software Subscription license to be eligible to download new releases of Check Point Security Gateway Appliances software, including hot fixes, service packs and major upgrades.

Note: The evaluated version is identified in section 1.2. The Check Point procedures for flaw remediation are included in the scope of the evaluation, but the configuration resulting from the application of a hot fix, service pack or major upgrade is not the evaluated configuration. However, it may be included in other Check Point evaluations.

1.5.4.5. 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 an Enterprise Support program are guaranteed a direct response, in accordance with their Service Level Agreement (SLA).

1.5.4.6. IPS Update Services

TOE users may purchase a recurring subscription to Check Point IPS Update Services. IPS Update Services are backed by the Check Point IPS 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 IPS 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). IPS Update Services provide Check Point customers with up-to-date defenses against new attacks.

IPS Updates are made available on the Check Point Web site for licensed customers. IPS Updates contain packaged IPS logic as described in section 1.5.3.8 above, allowing the authorized administrator to enable specific defenses against known attack signatures that have been identified by the IPS Research Center.

In addition, licensed IPS Update Services customers receive Security Best Practices and IPS 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 IPS Updates.

2. Conformance Claims

2.1. CC Conformance

The TOE is conformant with the following CC specifications:

- Common Criteria for Information Technology Security Evaluation Part 2: Security functional requirements, Version 3.1, Revision 4, September 2012, CCMB-2012-09-002, extended (CC Part 2 Extended)
- Common Criteria for Information Technology Security Evaluation Part 3: Security assurance requirements, Version 3.1 Revision 4, September 2012, CCMB-2012-09-003, conformant (CC Part 3 Conformant)

2.2. Assurance Package Conformance

The TOE is package-name augmented with the following assurance package:

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

2.3. PP Conformance

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

- U.S. Government Protection Profile for Traffic Filter Firewall In Basic Robustness Environments, Version 1.1, July 25, 2007
- U.S. Government Protection Profile for Application-level Firewall In Basic Robustness Environments, Version 1.1, July 25, 2007
- U.S. Government Protection Profile Intrusion Detection System System for Basic Robustness Environments, Version 1.7, July 25, 2007

2.4. Conformance Rationale

2.4.1. Introduction

This section is intended to demonstrate that the statements of the security problem definition, security objectives, and security requirements in this ST are consistent with the PPs for which conformance is being claimed: [TFF-PP], [APP-PP], and [IDSSPP].

All claimed protection profiles are CCv3.1 PPs that require demonstrable PP conformance.

Note: [TFF-PP] and [APP-PP] share many characteristics, including specification of identical security problem definition considerations, security objectives for the TOE and its IT environment, and SFRs, except for a few exceptions mostly relating to the user authentication and proxying requirements given in the latter PP. Where this ST refers to the 'firewall PPs', the reference relates to both [TFF-PP] and [APP-PP].

2.4.2. Consistency of the Security Problem Definition

The security problem definition in this ST is equivalent or more restrictive than the security problem definition of each of the claimed PPs. This is established as follows:

- This ST omits most of the assumptions defined in the claimed PPs. The omission of an assumption makes the security problem definition more restrictive[14] in that assumptions constrain the required security solution.
- All threats and OSPs defined in all claimed PPs are redefined in identical form in sections 3.1 and 3.3, respectively, except for [APP-PP] T.LOWEXP which as stated is in fact an assumption, and as such omitted from this ST. Section 3.1.4 and 3.1.5 define additional threats that are countered by the TOE's VPN and fault tolerance functionality. In relation to any of the individual claimed PPs, the definition of additional threats and OSPs serves to make the security problem definition more restrictive, and cannot cause inconsistency in of itself.

For each assumption defined in this ST, rationale is provided here for consistency with the defined environment of each of the claimed PPs:

A.LOCATE *The processing resources of the TOE will be located within controlled access facilities, which will prevent unauthorized physical access.*

This assumption is stated in identical form in [IDSSPP], and is consistent with the firewall PPs' A.PHYSEC assumption that "the TOE is physically secure".

[14] [CC] Part 1 Annex D explains that consistency of the SPD requires that all operational environments that would meet the security problem definition in the PP would also meet the security problem definition in the ST. This is achieved by providing rationale for each assumption defined in this ST that it is consistent with the defined environment of each of the claimed PPs, i.e. that any environment that would meet the assumptions in the PP would uphold the assumptions defined in this ST.

A.NOEVIL *Administrators are not careless, willfully negligent, or hostile, and will follow and abide by the instructions provided by the TOE documentation. However, they are capable of error.*

This assumption is a restrictive integration of the correspondingly-named [IDSSPP] and firewall PP assumptions, and is thus consistent with all three claimed PPs.

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

This assumption is stated in identical form in the firewall PPs.

It is equivalent to the [IDSSPP] A.ACCESS in the context of the TOE, in the sense that the IT System data collected by the TOE for the performance of its IDS functions is information flowing among the internal and external networks.

2.4.3. Security Objectives Conformance

The statement of security objectives in this ST was constructed as follows: the security objectives for the TOE include all firewall 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 subsection 2.4.3.1), or irrelevant in the context of this ST.

2.4.3.1. 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, i.e. of an inline gateway which mediates network information flows. 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 2-1 lists IT security objectives for the TOE defined in [IDSSPP] that have been omitted from this ST, providing rationale to justify their exclusion.

Table 2-1 - Omitted [IDSSPP] IT Security Objectives

[IDSSPP] objective	Equivalent in this ST	Omission rationale
O.IDSCAN	None – irrelevant as the TOE does not perform scanning;	The [IDSSPP] requires that a conformant TOE must include at least one Sensor or Scanner (see [IDSSPP] application note for IDS_SDC.1), but

[IDSSPP] objective	Equivalent in this ST	Omission rationale
	only sensing.	not both. The Check Point Security Gateway Appliances IDS provides a Sensor that inspects traffic flowing through the TOE, but does not actively scan protected hosts for vulnerabilities.
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 administrators may access such functionality.
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 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].

2.4.3.2. Security Objectives for the Environment

All three PPs for which conformance is claimed allocate security objectives for the IT and non-IT environment. Security objectives for the environment are traced to assumptions that must be upheld, and to threats that the TOE does not counter or threats that the TOE relies on cooperation from the environment for countering.

As described in section 2.4.2 above, this ST omits most of the assumptions made by the claimed PPs. The remaining assumptions defined in section 3.2 must be upheld by

suitable objectives for the environment. In addition, some TOE security mechanisms rely on the cooperation of the IT environment.

Table 2-2 provides consistency rationale for each stated environment security objective in relation to each of the claimed PPs. An environment security objective is considered consistent with a PP if it is identical[15] or equivalent to an environment security objective explicitly stated in that PP, a restrictive integration of two or more corresponding environment security objectives from the claimed PPs, if it is consistent with the implicit assumptions of the PP, and if it does not serve to violate the original intent of the assumptions of the PP[16].

Table 2-2 - PP Conformance and Environment Security Objectives

Objective	[TFF-PP] and [APP-PP]	[IDSSPP]
NOE.INSTALL	Equivalent to O.GUIDANCE	Identical to OE.INSTAL
NOE.ADMTRA	Restrictive integration of the firewall PPs' O.ADMTRA[17] with the [IDSSPP] OE.PERSON.	
NOE.PHYSICAL	Equivalent to A.PHYSEC	Identical to OE.PHYCAL
NOE.CREDEN	While not explicitly stated in [TFF-PP] or [APP-PP], it should be applicable to these PPs as well, and does not serve to violate the original intent of the Firewall PP assumptions.	Identical to O.CREDEN
OE.SINGEN	Equivalent to A.SINGEN	See consistency rationale for A.SINGEN in section 2.4.2.
OE.IDAUTH	Demonstrably consistent in accordance with the guidance given in [PD-0115].	Demonstrably consistent in accordance with the guidance given in [PD-0151].
	In particular, the TSF implements the user authentication function, and can authenticate users without relying on an authentication server in the IT environment, using certificate-based authentication. As stated in [PD-0151], "it should be possible to be able to support not only local authentication, but authentication via a LDAP or Radius server in the operational environment (which provides support for the DOD 8500.2 DCBP control).	
OE.VPN	The TOE's VPN functionality is additional security functionality that is not required to address any of the threats or assumptions made in any of the claimed PPs. While this functionality depends on the VPN peer's enforcement of a compatible security policy, this does not serve to violate any of the original intent of the claimed PPs' assumptions.	
OE.VLAN	The rationale for consistency with the claimed PPs is similar to the rationale given above for OE.IDAUTH. OE.VLAN supports the user authentication function by relying on an external IT entity to securely provide the user's logical identity. The TOE can perform this function without relying	

[15] 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.

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

[17] Note that the NOE.ADMTRA is also consistent with firewall PP objective for the environment A.NOEVIL, in the sense that careful administrator selection is meant to determine that they are non-hostile, and administrator training contributes to their following of all administrator guidance.

Objective	[TFF-PP] and [APP-PP]	[IDSSPP]
	on the IT environment if so configured (by binding users to subjects based on the physical rather than logical interface over which their requests are received by the TOE). VLAN-tagging is thus an additional security function supported by the TOE that does not violate the original intent of the claimed PPs' assumptions.	

2.4.4. Security Functional Requirements Conformance

2.4.4.1. Overview

The TOE demonstrably meets and exceeds all security requirements of all three PPs listed in section 2: [TFF-PP], [APP-PP], and [IDSSPP], except for the FIA_AFL.1, FIA_SOS.1, and FMT_MTD.2 requirements that are inapplicable to the TOE (see rationale below).

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 6-1.

The following subsections provide conformance rationale for individual SFRs that were omitted as exceptions or refined in respect to the claimed PPs, clarifying the relationship of an SFR to the claimed PPs.

2.4.4.2. FAU_GEN.1

FAU_GEN.1 has been derived from all claimed PPs.

This requirement has been refined in relation to all claimed PPs, to include a superset of the corresponding requirement in each PP.

The set of auditable events includes all events from all claimed PPs, with the addition of events corresponding to other SFRs in this ST that were not drawn from these PPs. The level of audit in FAU_GEN.1.1 subsection b) is given as 'not specified', as defined in [APP-PP]. This is also consistent with both [TFF-PP] and [IDSSPP], each explicitly providing a table listing the applicable auditable events for the PP. [IDSSPP] also includes the requirement for auditing 'Access to the System and access to the TOE and System data' as an assignment for *other specifically defined auditable events* – this is specified here by the FAU_GEN.1 entries in Table 6-2.

Table 6-2 was constructed to include required auditable events and audit record contents from all claimed PPs. [CC] Part 2 was used as guidance for the selection of auditable events for SFRs that were not derived from any of the claimed PPs.

For FIA_UAU.1 as an auditable event, 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].

The entry for FPT_STM.1 as an auditable event given in [TFF-PP] and [APP-PP] has been omitted from this ST. FMT_MOF.1has been refined to restrict the setting of the time and date to no administrator role 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.

2.4.4.3. FAU_SAR.3

FAU_SAR.3 has been derived from all claimed PPs.

FAU_SAR.3 has been updated to CCv3.1 Part 2 syntax, with assignments 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). Highlighting conventions are applied in relation to the original CCv3.1 Part 2 component.

2.4.4.4. FAU_STG.2

The [IDSSPP] FAU_STG.2 component has been selected because it is hierarchical to the Firewall PPs' FAU_STG.1. It was refined to conform with CCv3.1 syntax. This is also consistent with [I-0422].

In FAU_STG.2.2, the selection is given as 'prevent' from the Firewall PPs as it is stronger than 'detect' given in [IDSSPP].

2.4.4.5. FCS_COP.1 /Admin

FCS_COP.1 /Admin is drawn from the [TFF-PP]. The original syntax adds: “(as specified in SP 800-67)]”. This is apparently a carry-over from a previous version of the PP, as SP 800-67 defines the Triple DES encryption algorithm. The updated PP requires AES (as specified in FIPS 197) instead of Triple DES. Because it is an error in the PP, the omission of this specification has not been identified as a refinement in relation to the PP.

2.4.4.6. FDP_IFC.1 /TFF

FDP_IFC.1 /TFF has been drawn from [TFF-PP]

Both protection profiles [APP-PP] and [TFF-PP] specify an SFP identified as UNAU-THENTICATED 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/TFF and FDP_IFF.1/TFF, 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.

The original [TFF-PP] UNAUTHENTICATED SFP is refined here to allow traffic filtering for authenticated external IT entities (see also section 6.1.4.3). This is consistent with [TFF-PP] because it is more restrictive.

According to the subject/object model described in [CC], an external IT entity is a *user*, not a *subject*, as a subject is defined as an active entity in the TOE. The external IT entity (U.USER or U.RAUSER or U.VPNPEER) binds to a TOE subject (S.VS), which performs operations on information (D.INFO) in the form of IPv4 packets (D.PACKET) on its behalf. The original [TFF-PP] syntax is used here for enhanced readability and for consistency with the PP, describing information flows as occurring between external IT entities.

2.4.4.7. FDP_IFC.1 /UNAUTH

FDP_IFC.1 /UNAUTH has been derived from [APP-PP].

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/TFF and FDP_IFF.1/TFF, 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.

2.4.4.8. FDP_IFF.1 /UNAUTH

FDP_IFF.1 /UNAUTH has been derived from [APP-PP].

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/UNAUTH 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/UNAUTH.

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].

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].

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.

2.4.4.9. FDP_IFF.1 /AUTH

FDP_IFF.1 /AUTH has been derived from [APP-PP].

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/AUTH 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/AUTH

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].

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.

2.4.4.10. FDP_IFF.1 /TFF

FDP_IFF.1 /TFF has been derived from [TFF-PP].

Elements FDP_IFF.1.2 and FDP_IFF.1.5 were refined in accordance with [PD-0036] to remove the distinction made in [TFF-PP] between internal and external networks, replacing it with a concept of association of sets of source subject identifiers (IP addresses) with logical interfaces, as expressed in [PPFWTFMR].

FDP_IFF.1.3 is expressed in [TFF-PP] using the older CCv2.1 syntax, in two separate elements, both completed with the assignment [none]. The corresponding element in this ST is refined to use the five-element CCv3.1 syntax, and to describe additional TOE security capabilities applied as part of traffic filtering, including de-fragmentation and stateful packet inspection (derived from the more-restrictive [PPFWTFMR] Protection Profile), and NAT.

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.

2.4.4.11. FDP_RIP.2

FDP_RIP.2 has been derived from [TFF-PP] and [APP-PP].

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.

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.

2.4.4.12. FIA_AFL.1

The FIA_AFL.1 requirement appearing in [TFF-PP], [APP-PP], and [IDSSPP] has been omitted from this ST. FIA_AFL.1 requires that an account lockout mechanism be in place that prevents external IT entity access after an administrator-defined number of unsuccessful authentication events. In the TOE evaluated configuration, external IT entities authenticate to the TOE using certificate-based or single-use authenticator-based authentication mechanisms, rather than via reusable 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.

2.4.4.13. FIA_ATD.1

FIA_ATD.1 has been derived from all claimed PPs.

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].

2.4.4.14. FIA_UAU.1

FIA_UAU.1 is specified here as being drawn from [IDSSPP] and [TFF-PP] because it is missing in the requirements of [APP-PP]. However, note that it is a dependency of FIA_AFL.1 which appears in [APP-PP]. 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.

FIA_UAU.1 is presented using [IDSSPP] syntax. This is a refinement of the corresponding [TFF-PP] SFR, which assigns the list of TSF mediated actions in FIA_UAU.1.1 as ‘identification as stated in FIA_UID.2’, and refines ‘user’ to ‘authorized administrator or authorized external IT entity accessing the TOE’, i.e. the only authenticated users in the context of [TFF-PP]. The pre-authentication actions identified here are all consistent with the [TFF-PP] requirement that a U.ADMIN and U.AIETE user must identify and authenticate prior to performing any TSF-mediated actions.

2.4.4.15. FIA_UAU.5

FIA_UAU.5 has been derived from [APP-PP].

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 used for authorized administrators to access the TOE via a directly connected terminal has been omitted because a directly connected terminal is not used in the evaluated configuration.

2.4.4.16. FMT_MOF.1

FMT_MOF.1 has been derived from all claimed PPs.

FMT_MOF.1 is stated differently in [TFF-PP] than in [APP-PP] or [IDSSPP]. [TFF-PP] lists all management operations in this SFR, restricting them to the single authorized administrator role defined in that PP, and leaving an assignment for the ST writer(s) to fill in additional security-relevant administrative functions. [APP-PP] and [IDSSPP] take a different approach, using multiple iterations of FMT_MSA.1, FMT_MTD.1, and FMT_MOF.1 to express management restrictions, leaving no open assignment. This ST lists all security management functions and restrictions to roles in the context of FMT_SMF.1, and refines FMT_MOF.1 (and FMT_MTD.1) to refer to FMT_SMF.1. The assignment operation identified here is in relation to [TFF-PP]. All management operations identified in all claimed PPs are included in this ST.

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. FMT_MOF.1 restricts the setting of the time and date after the TOE is operational to no administrator role. This can be considered more secure than restricting this function to the authorized administrator, and is therefore consistent with the intention of the claimed PPs. As a consequence of this refinement, the auditable event in FAU_GEN.1 for an administrator change of the time and date was removed.

2.4.4.17. FMT_MSA.1

FMT_MSA.1 is stated as four iterations in [APP-PP], with the first two iterations restricting the ability to manage rule attributes for the UNAUTHENTICATED SFP and AUTHENTICATED SFP, respectively, and the second two iterations use to restrict management of the rules themselves for these two SFPs. This ST states these requirements in two iterations, for restricting management of rule attributes, and for rules, including both [APP-PP] SFPs, as well as the [TFF-PP] UNAUTHENTICATED SFP (identified here as TRAFFIC FILTER SFP).

2.4.4.18. FMT_MTD.1

FMT_MTD.1 been derived from [IDSSPP] and [APP-PP].

This SFR is refined in relation to both [IDSSPP] and [APP-PP], to incorporate the FMT_MTD.1 iterations from these PPs in Table 6-3. This is consistent with the approach

taken in [TFF-PP] for FMT_MOF.1, and does not modify the intent of the original SFRs. Highlighting for this SFR is performed in relation to the [CC] Part 2 component.

As explained above for FMT_MOF.1, FMT_MTD.1 restricts the setting of the time and date after the TOE is operational to no administrator role. This can be considered more secure than restricting this function to the authorized administrator, and is therefore consistent with the intention of the claimed PPs.

2.4.4.19. FMT_MTD.2

See above, rationale for omitting FIA_AFL.1 from this ST.

2.4.4.20. FMT_SMR.1

FMT_SMR.1 has been derived from all claimed PPs.

The syntax, semantics, and highlighting convention for FMT_SMR.1 is applied in relation to [IDSSPP], which differentiates between the authorized administrator and authorized System administrator roles, and allows additional authorized identified roles. [TFF-PP] and [APP-PP] both define a single ‘authorized 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.

2.4.4.21. FPT_STM.1

FPT_STM.1 has been derived from all claimed PPs.

FPT_STM.1 was refined (in relation to the claimed PPs) to conform with CCv3.1 syntax, omitting the phrase “for its own use”.

2.4.4.22. Applicable NIAP Precedent Decisions

The following precedent decisions have been used as guidance for interpreting the claimed PPs:

Table 2-3- References to Guidance on the Interpretation of Claimed PPs

Reference	Affected PPs	Affected SFRs and objectives	Description
[PD-0018]	[TFF-PP], [APP-PP]	FDP_IFF.1	The term "loopback address" is to be used in place of "loopback network"
[PD-0055]	All	Objectives for the environment	Additional assumptions are allowed if they do not violate the intent of the PP

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]	FIA_UAU.5	IKE authentication is acceptable as "single use"
[PD-0115]	[TFF-PP], [APP-PP]	O.IDAUTH, FIA_UID.2, FIA_UAU.5	Moved to the environment to support use of external authentication servers

2.4.5. Security Assurance Requirements Conformance

All claimed PPs require a minimum assurance level of EAL 2, augmented with ALC_FLR.2.

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. The assurance requirements in this ST are therefore clearly hierarchically stronger than the ones required by the claimed PPs.

3. Security Problem Definition

.

3.1. Threats

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 and fault tolerance functionality.

3.1.1. 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.

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.TUSAGE The TOE may be inadvertently configured, used, and administered in an insecure manner by either authorized or unauthorized persons.

3.1.2. IDS-related Threats

The following threats are identified in [IDSSPP] (provided here for the benefit of the reader of the ST). Note that the IT System that the TOE monitors is the network, and indirectly the resources on the network.

Application Note: *The [IDSSPP] identifies three threats that are to be defined only if the TOE contains a Scanner: T.SCNCFG, T.SCNMLC, and T.SCNVUL. As the TOE does not contain a Scanner, these threats have not been included in this ST.*

T.COMINT An unauthorized user may attempt to compromise the integrity of the data collected and produced by the TOE by bypassing a security mechanism.

T.COMDIS An unauthorized user may attempt to disclose the data collected and produced by the TOE by bypassing a security mechanism.

T.LOSSOF An unauthorized user may attempt to remove or destroy data collected and produced by the TOE.

T.NOHALT An unauthorized user may attempt to compromise the continuity of the System's collection and analysis functions by halting execution of the TOE.

T.PRIVIL An unauthorized user may gain access to the TOE and exploit system privileges to gain access to TOE security functions and data

T.IMPCON An unauthorized user may inappropriately change the configuration of the TOE causing potential intrusions to go undetected.

T.INFLUX An unauthorized user may cause malfunction of the TOE by creating an influx of data that the TOE cannot handle.

T.FACCNT Unauthorized attempts to access TOE data or security functions may go undetected.

T.FALACT The TOE may fail to react to identified or suspected vulnerabilities or inappropriate activity.

T.FALREC The TOE may fail to recognize vulnerabilities or inappropriate activity based on IDS data received from each data source.

T.FALASC The TOE may fail to identify vulnerabilities or inappropriate activity based on association of IDS data received from all data sources.

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.

3.1.3. Virtualization-related Threats

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

T.ACCESS An unauthorized person or external IT entity may be able to access data flowing through or stored within the TOE in violation of Virtual System domain separation policy.

3.1.4. 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.

3.1.5. Fault-related Threats

The following threat is countered by the TOE's fault tolerance functionality.

T.FAULT A failure in a critical hardware or software entity may disrupt TOE security functions.

3.2. Assumptions

The following conditions are assumed to exist in the operational environment. As demonstrated in section 2.4.2 above, each of these assumptions is consistent with the explicit or implicit assumptions made in each of the PPs for which conformance is claimed: [TFF-PP], [APP-PP], and IDSSPP].

A.LOCATE The processing resources of the TOE will be located within controlled access facilities, which will prevent unauthorized physical access.

A.NOEVIL Administrators are not careless, willfully negligent, or hostile, and will follow and abide by the instructions provided by the TOE documentation. However, they are capable of error.

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

3.3. Organizational Security Policies

3.3.1. Firewall PP OSPs

The [APP-PP] defines the following OSP[18]:

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 AES (Advanced Encryption Standard as specified in FIPS 197) encryption must be used to protect remote administration functions, and the associated cryptographic module must comply, at a minimum, with FIPS 140-2 (level 1).

3.3.2. IDS System PP OSPs

The following OSPs are defined in [IDSSPP]. [IDSSPP] does not identify which organization and which organizational security policy any of these OSPs are drawn from.

P.DETECT Static configuration information that might be indicative of the potential for a future intrusion or the occurrence of a past intrusion of an IT System or events that are indicative of inappropriate activity that may have resulted from misuse, access, or malicious activity of IT System assets must be collected.

P.ANALYZ Analytical processes and information to derive conclusions about intrusions (past, present, or future) must be applied to IDS data and appropriate response actions taken.

P.MANAGE The TOE shall only be managed by authorized users.

P.ACCESS All data collected and produced by the TOE shall only be used for authorized purposes.

P.ACCACT Users of the TOE shall be accountable for their actions within the IDS.

P.INTGTY Data collected and produced by the TOE shall be protected from modification.

P. PROTCT The TOE shall be protected from unauthorized accesses and disruptions of TOE data and functions.

[18] The [APP-PP] P.CRYPTO text adds the following term: '(as specified in SP 800-67)'. This is apparently a carry-over from a previous version of the PP, as explained in Section 2.4.4.5, and has been omitted in this ST.

3.3.3. Virtualization OSPs

The following OSP is defined in this ST to require compartmentalization of data within the TOE.

P.VIRTUAL The TOE shall enforce separation between Virtual Systems and allow controlled sharing of information.

4. Security Objectives

4.1. Security Objectives for the TOE

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 and fault tolerance 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 ‘with the support of the IT environment’ has been added to the definition of O.IDAUTH to support the optional use by the TSF of authentication mechanisms that rely on IT environment support, e.g. RADIUS authentication servers. This is consistent with the guidance given by [PD-0115]. A corresponding objective for the IT environment OE.IDAUTH has been added to the ST to reflect this split of functionality between the TOE and its IT environment.
- 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.
- O.EAL was defined in [APP-PP] mapping to T.LOWEXP. T.LOWEXP has been omitted from this ST, as explained in section 2.4.2. Since O.EAL is an objective for the development environment of the TOE rather than for the TOE itself, it may be omitted without violating demonstrable conformance with the PP.

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 and data or, for certain specified services, to a connected network.

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.

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 in section 2.4.3.1 that have been omitted in this ST because they are not needed to establish the [IDSSPP] IT security requirements:

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

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.

4.1.4. Virtualization Objectives

O.MAC The TOE must control access to resources in accordance with Virtual System domain separation rules based on the labeling of subjects and of the information being accessed.

4.1.5. Fault Tolerance Objectives

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

O.FAULT The TOE must be able to ensure that TOE security functions function correctly after a failure of a critical hardware or software entity

4.2. Security Objectives for the Operational Environment

4.2.1. Security Objectives for the Environment Upholding Assumptions

The assumptions made in this ST about the TOE's operational environment must be upheld by corresponding security objectives for the environment.

The following security objectives are intended 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.INSTALL Those responsible for the TOE must ensure that the TOE is delivered, installed, managed, and operated in a manner which is consistent with IT security.

NOE.ADMTRA Personnel working as administrators shall be carefully selected and trained for proper operation of the System and the establishment and maintenance of security policies and practices.

NOE.PHYSICAL Those responsible for the TOE must ensure that those parts of the TOE critical to security policy are protected from any physical attack.

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.

OE.SINGEN Those responsible for the TOE must ensure that information can not flow among the internal and external networks unless it passes through the TOE.

4.2.2. Authentication Security Objectives for the IT Environment

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.

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.

4.2.3. VPN Security Objectives for the IT Environment

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.

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.

Note: As described in sections 1.5.1.7 and 1.5.1.8, the underlying platform for TOE SSL VPN clients, and the platform and software for compatible IPsec VPN clients are all considered to be outside the boundaries of the TOE.

The TOE’s claimed security functionality includes identification and authentication of the remote access VPN user, and support for trusted channel establishment. The TOE does not rely on the integrity of the client platform for the enforcement of its SFRs. However, the TOE does not protect user data or cryptographic keys stored on the client. Compromise of the client platform may allow an attacker to access and/or modify information flowing through the TOE to and from the client, without due authorization; this might be considered to be undesirable by users of the TOE.

Users should therefore take care that the underlying operating system and hardware used for running remote access VPN clients is protected from tampering and interference, using additional security mechanisms that are outside the boundaries of the TOE. For example, the Check Point Endpoint Security product (evaluated separately) provides a wide range of security functionality that may be used to protect the client platform against network-based attacks, malware, removable media devices, unauthorized physical access threats, and more.

4.2.4. VLAN Security Objectives for the IT Environment

The TOE identifies and authenticates users based on the logical interface through which their requests (IPv4 packets) flow into the TOE, and binds the user to a corresponding subject (Virtual System) based on this identification. Where the logical interface corresponds to a physical interface, the TSF uses physical authentication.

The TOE can be configured to support VLAN-tagging in order to determine the logical interface. In this case, the TOE depends on the physically connected switch device to support identification and authentication by correctly labeling incoming traffic with the appropriate VLAN tag.

The IT environment is responsible for protecting channel data from modification or disclosure outside the TOE. Where the switch device is co-located with the TOE, this is often achieved by physical security measures. Where they are widely separated, those responsible for the TOE should consider using additional cryptographic security measures in the IT environment to protect the channel data.

OE.VLAN	The IT environment must be able to provide logically distinct VLAN-tagged communication channels with the TOE that provide assured endpoint identification and protection of channel data from modification or disclosure outside of the TOE.

4.3. Security Objectives Rationale

The [TFF-PP] and [APP-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 and fault tolerance-related security objectives (no PP conformance claimed) were added to the ST. The following subsections describe how these objectives were mapped to security environment considerations.

4.3.1. Security Objectives Countering Threats

Table 4-1, Table 4-2, Table 4-3, and Table 4-5 each map the security objectives defined in this ST to threats defined in sections 3.1.1, 3.1.2, 3.1.4, and 3.1.5 respectively, for Firewall PP, [IDSSPP], VPN, and fault-related threats. In each table, mapped threats and objectives are identified in **boldface**. Together, the tables clearly demonstrate that each threat is countered by at least one security objective and that each TOE objective counters at least one threat.

Each table is accompanied by explanatory text providing justification for each defined threat that if all security objectives that trace back to the threat are achieved, the threat is removed, sufficiently diminished, or that the effects of the threat are sufficiently mitigated. Where the tracing of security objectives to threats is directly derived from a claimed Protection Profile, the justification is by reference to the security objectives rationale in the PP.

4.3.1.1. Firewall PP Threats

The mapping of the Firewall PP IT security objectives (O.IDAUTH through O.LIMEXT) and of the NOE.INSTALL and NOE.ADMTRA objectives to environmental considerations is identical[15] to the mapping given in [TFF-PP] and [APP-PP]. OE.IDAUTH was added tracing to T.NOAUTH, in accordance with the guidance given in [PD-0115].

Table 4-1 -Tracing of security objectives to [TFF-PP] and [APP-PP] threats

	T.NOAUTH	T.REPEAT	T.REPLAY	T.ASPOOF	T.MEDIAT	T.OLDINF	T.PROCOM	T.AUDACC	T.SELPRO	T.AUDFUL	T.TUSAGE
O.IDAUTH	✓										
O.SINUSE		✓	✓								
O.MEDIAT				✓	✓	✓					
O.SECSTA	✓								✓		
O.ENCRYP	✓						✓				

	T.NOAUTH	T.REPEAT	T.REPLAY	T.ASPOOF	T.MEDIAT	T.OLDINF	T.PROCOM	T.AUDACC	T.SELPRO	T.AUDFUL	T.TUSAGE
O.SELPRO	✓								✓	✓	
O.AUDREC								✓			
O.ACCOUN								✓			
O.SECFUN	✓		✓							✓	
O.LIMEXT	✓										
O.PROTCT	✓								✓		
O.IDSENS					✓						
O.IDANLZ					✓						
O.RESPON					✓						
O.OFLOWS										✓	
O.INTEGR									✓		
O.MAC											
O.VPN											
O.FAULT											
NOE.INSTALL											✓
NOE.ADMTRA											✓
NOE.PHYSICAL											
NOE.CREDEN											
OE.SINGEN											
OE.IDAUTH	✓										
OE.VPN											
OE.VLAN											

Some [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.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.*

O.PROTCT supports O.SELPRO by requiring protection against unauthorized modifications and access to TOE functions and data.

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 [TFF-PP]and [APP-PP], 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 [TFF-PP] and [APP-PP] 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, and O.PROTCT requires protection against unauthorized modifications and access to TOE functions and data.

4.3.1.2. IDS PP threats

The mapping of security objectives to [IDSSPP] environmental considerations was directly derived from [IDSSPP] by replacing each [IDSSPP] security objective with its counterpart in this ST, as identified in section 4.1.2.

OE.IDAUTH was added tracing to the threats mapped in [IDSSPP] to O.IDAUTH, consistently with the guidance given in [PD-0151].

Table 4-2 -Tracing of security objectives to [IDSSPP] threats

	T.COMINT	T.COMDIS	T.LOSSOF	T.NOHALT	T.PRIVIL	T.IMPCON	T.INFLUX	T.FACCNT	T.FALACT	T.FALREC	T.FALASC	T.MISUSE	T.INADVE	T.MISACT
O.IDAUTH	✓	✓	✓	✓	✓	✓								
O.SINUSE														
O.MEDIAT														

	T.COMINT	**T.COMDIS**	**T.LOSSOF**	**T.NOHALT**	**T.PRIVIL**	**T.IMPCON**	**T.INFLUX**	**T.FACCNT**	**T.FALACT**	**T.FALREC**	**T.FALASC**	**T.MISUSE**	**T.INADVE**	**T.MISACT**
O.SECSTA														
O.ENCRYP														
O.SELPRO														
O.AUDREC								✓				✓	✓	✓
O.ACCOUN														
O.SECFUN	✓	✓	✓	✓	✓	✓								
O.LIMEXT														
O.PROTCT	✓	✓	✓		✓									
O.IDSENS				✓								✓	✓	✓
O.IDANLZ				✓						✓	✓			
O.RESPON									✓					
O.OFLOWS							✓							
O.INTEGR	✓		✓											
O.MAC														
O.VPN														
O.FAULT														
NOE.INSTALL						✓								
NOE.ADMTRA														
NOE.PHYSICAL														
NOE.CREDEN														
OE.SINGEN														
OE.IDAUTH	✓	✓	✓	✓	✓	✓								
OE.VPN														
OE.VLAN														

4.3.1.3. VPN related threats

Table 4-3 -Tracing of security objectives to VPN related threats

	T.NACCESS	**T.NMODIFY**
O.IDAUTH		
O.SINUSE		
O.MEDIAT		
O.SECSTA		
O.ENCRYP		
O.SELPRO		
O.AUDREC		
O.ACCOUN		
O.SECFUN		
O.LIMEXT		
O.PROTCT		
O.IDSENS		
O.IDANLZ		
O.RESPON		
O.OFLOWS		
O.INTEGR		
O.MAC		
O.VPN	✓	✓
O.FAULT		
NOE.INSTALL		
NOE.ADMTRA		
NOE.PHYSICAL		
NOE.CREDEN		
OE.SINGEN		
OE.IDAUTH		
OE.VPN	✓	✓
OE.VLAN		

The description of the TOE security environment introduces two additional threats on top of the firewall PP-defined threats, in section 3.1.2, 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.

4.3.1.4. Virtualization-related Threats

Table 4-4 -Tracing of security objectives to Virtualization related threats

	T. ACCESS
O.IDAUTH	
O.SINUSE	
O.MEDIAT	✓
O.SECSTA	
O.ENCRYP	
O.SELPRO	
O.AUDREC	
O.ACCOUN	
O.SECFUN	
O.LIMEXT	
O.PROTCT	
O.IDSENS	
O.IDANLZ	
O.RESPON	
O.OFLOWS	
O.INTEGR	
O.MAC	✓
O.VPN	
O.FAULT	
NOE.INSTALL	
NOE.ADMTRA	
NOE.PHYSICAL	
NOE.CREDEN	
OE.SINGEN	
OE.IDAUTH	
OE.VPN	
OE.VLAN	✓

The description of the TOE security environment introduces an additional threat that is countered by the TOE's Virtualization IT security functionality:

T.ACCESS *An unauthorized person or external IT entity may be able to access data flowing through or stored within the TOE in violation of Virtual System domain separation policy.*

This threat is countered by O.MAC which requires the TOE to restrict access to data flowing through the TOE, or stored withn the TOE, respectively, in accordance with Virtual System domain separation rules based on the labeling of subjects and of the information being accessed.

O.MEDIAT supports O.MAC by requiring that all information flowing through the TOE must be mediated by the TOE, preventing any information from flowing between multiple virtual enclaves without appropriate authorization. O.MEDIAT also prevents leakage of residual information. OE.VLAN supports O.MAC by labeling information flowing through the TOE with VLAN tags that are used to determine the labels used in enforcing O.MAC.

4.3.1.5. Fault related threats

Table 4-5 -Tracing of security objectives to Fault related threats

	T.FAULT
O.IDAUTH	
O.SINUSE	
O.MEDIAT	
O.SECSTA	
O.ENCRYP	
O.SELPRO	
O.AUDREC	
O.ACCOUN	
O.SECFUN	
O.LIMEXT	
O.PROTCT	
O.IDSENS	
O.IDANLZ	
O.RESPON	
O.OFLOWS	
O.INTEGR	
O.MAC	
O.DAC	
O.VPN	
O.FAULT	✓
NOE.INSTALL	
NOE.ADMTRA	
NOE.PHYSICAL	
NOE.CREDEN	
OE.SINGEN	
OE.IDAUTH	
OE.VPN	
OE.VLAN	

The description of the TOE security environment introduces an additional threat that is countered by the TOE's fault tolerance IT security functionality:

T.FAULT *A failure in a critical hardware or software entity may disrupt TOE security functions.*

This threat is directly countered by O.FAULT, which requires that the TOE be able to ensure that TOE security functions function correctly after a failure of a critical hardware or software entity.

4.3.2. Security Objectives Upholding OSPs

Table 4-6 maps security objectives to the organizational security policies described in chapter 3. The table clearly demonstrates that each security policy is countered by at least one security objective. The rationale for this mapping is given in [IDSSPP], in relation to the [IDSSPP] security objectives mapped in section 4.1.2, and in [APP-PP] for the mapping of O.ENCRYP to the P.CRYPTO OSP defined in that PP. The table also maps the P.VIRTUAL OSP defined in this ST to security objectives, with the same mapping and rationale given above for T.ACCESS.

OE.IDAUTH was added tracing to the OSPs mapped in [IDSSPP] to O.IDAUTH. See section 2.4.3.2 above for a rationale of why this is consistent with the intent of this PP.

Table 4-6 -Tracing of security objectives to OSPs

	P.CRYPTO	P.DETECT	P.ANALYZ	P.MANAGE	P.ACCESS	P.ACCACT	P.INTGTY	P.PROTCT	P.VIRTUAL
O.IDAUTH				✓	✓	✓			
O.SINUSE									
O.MEDIAT									✓
O.SECSTA									
O.ENCRYP	✓								
O.SELPRO									
O.AUDREC[19]		✓				✓			
O.ACCOUN									
O.SECFUN				✓	✓				
O.LIMEXT									
O.PROTCT[20]				✓	✓				

[19] O.AUDREC subsumes the [IDSSPP] OE.TIME and OE.AUDIT_SORT security objectives for the environment, by ensuring that the TOE records accurate dates and times in the audit trail, and provides a means to sort the audit trail based on relevant attributes.

	P.CRYPTO	P.DETECT	P.ANALYZ	P.MANAGE	P.ACCESS	P.ACCACT	P.INTGTY	P.PROTCT	P.VIRTUAL
O.IDSENS		✓							
O.IDANLZ			✓						
O.RESPON									
O.OFLOWS								✓	
O.INTEGR							✓		
O.MAC									✓
O.VPN									
O.FAULT									
NOE.INSTALL[21]				✓					
NOE.ADMTRA				✓					
NOE.PHYSICAL								✓	
OE.CREDEN				✓					
OE.SINGEN									
OE.IDAUTH				✓	✓	✓			
OE.VPN									
OE.VLAN									✓

4.3.3. Security Objectives Upholding Assumptions

Table 4-7 maps security objectives for the operational environment to assumptions made in section 3.2. Each assumption traces to corresponding security objectives, derived from the claimed PPs in accordance with the mapping to PP assumptions in section 2.4.2. The table demonstrates that each assumption is upheld by at least one security objective for the environment. Together with the preceding tables in this chapter, it can be clearly seen that each security objective for the environment is traced to at least one environment consideration.

---

[20] O.PROTCT also subsumes the [IDSSPP] OE.AUDIT_PROTECTION security objective for the environment (mapped in [IDSSPP] to P.ACCESS), as the audit trail is stored within the TOE.

[21] The [IDSSPP] security objectives for the environment were mapped to the following environment objectives in this ST (see Table 2-2 for additional rationale):

- OE.INSTAL – renamed NOE.INSTALL in this ST.
- OE.PHYCAL – equivalent to NOE.PHYSICAL in this ST.
- OE.CREDEN – renamed NOE.CREDEN in this ST.
- OE.PERSON – integrated into NOE.ADMTRA.

Table 4-7- Tracing of Security Objectives Upholding Assumptions

	A.LOCATE	**A.NOEVIL**	**A.SINGEN**
O.IDAUTH			
O.SINUSE			
O.MEDIAT			
O.SECSTA			
O.ENCRYP			
O.SELPRO			
O.AUDREC			
O.ACCOUN			
O.SECFUN			
O.LIMEXT			
O.PROTCT			
O.IDSENS			
O.IDANLZ			
O.RESPON			
O.OFLOWS			
O.INTEGR			
O.MAC			
O.VPN			
O.FAULT			
NOE.INSTALL		[IDSSPP]	
NOE.ADMTRA			
NOE.PHYSICAL	[IDSSPP]	[IDSSPP]	
OE.CREDEN		[IDSSPP]	
OE.SINGEN			[TFF-PP], [APP-PP]
OE.IDAUTH			
OE.VPN			
OE.VLAN			

5. Extended Components Definition

This security target contains the following extended security requirements defined in [IDSSPP]: IDS_SDC(EXP).1, IDS_ANL(EXP).1, IDS_RCT(EXP).1, IDS_RDR(EXP).1, IDS_STG(EXP).1, IDS_STG(EXP).2**.**

Extended security functional requirements are not drawn from [CC] Part 2 components. The [IDSSPP] provides the following explanation for why these requirements cannot be clearly expressed using existing components, and in particular why the FAU class could not be refined to achieve the same result. Note that FAU deals with events that are internal to the TOE, whereas IDS deals with events occurring in the IT environment.

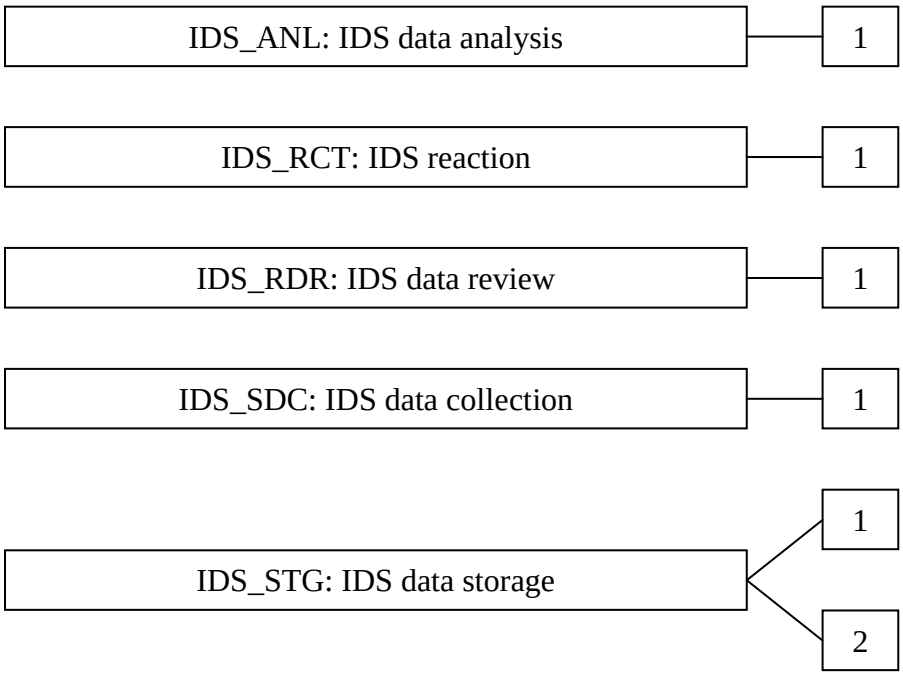
> "*A family of IDS requirements was created to specifically address the data collected and analyzed by an IDS. The audit family of the CC (FAU) was used as a model for creating these requirements. The purpose of this family of requirements is to address the unique nature of IDS data and provide for requirements about collecting, reviewing and managing the data.*"

The Extended Components Definition presented here defines an extended component for each extended security requirement, using the existing CC components, families, classes, and methodology as a model for presentation.

5.1. Class IDS: Intrusion Detection

This class is used to satisfy security objectives that pertain to intrusion detection and prevention (IDS/IPS) systems. These include data collection and analysis, automatic reaction capabilities, review, and protection of IDS System data.

Figure 5-1 - IDS: Intrusion detection class decomposition



5.1.1. IDS data analysis (IDS_ANL)

Family Behaviour

This family defines requirements for automated means that analyse IDS System data looking for possible or real security violations.

The actions to be taken based on the detection can be specified using the IDS reaction (IDS_RCT) family as desired.

Component levelling

IDS_ANL: IDS data analysis	1

In IDS_ANL.1 Analyser analysis, statistical, signature, or integrity based analysis is required.

Management: IDS_ANL.1

The following actions could be considered for the management functions in FMT:

a) maintenance (deletion, modification, addition) of the parameters of the analytical functions.

Audit: IDS_ANL.1

The following actions should be auditable if IDS_ANL IDS data analysis is included in the PP/ST:

a) Minimal: Enabling and disabling of any of the analysis mechanisms.

5.1.1.1. IDS_ANL.1 Analyser analysis

Hierarchical to: No other components.

Dependencies: IDS_SDC.1 System data collection

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

a) [selection: *statistical*, *signature*, *integrity*]; and

b) [assignment: *any other analytical functions*].

IDS_ANL.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; and

b) [assignment: *any other security relevant information about the result*].

5.1.2. IDS reaction (IDS_RCT)

Family Behaviour

This family defines the response to be taken in case when an intrusion is detected.

Component levelling

IDS_RCT: IDS reaction	1

At IDS_RCT.1 IDS reaction, the TSF shall send an alarm and take action when an intrusion is detected.

Management: IDS_RCT.1

The following actions could be considered for the management functions in FMT:

a) the management (addition, removal, or modification) of actions.

Audit: IDS_RCT.1

The following actions should be auditable if IDS_RCT IDS reaction is included in the PP/ST:

a) Minimal: Actions taken due to detected intrusions.

5.1.2.1. IDS_RCT.1 Analyser react

Hierarchical to: No other components.

Dependencies: IDS_ANL.1 Analyser analysis

IDS_RCT.1.1 The System shall send an alarm to [assignment: *alarm destination*] and take [assignment: *appropriate actions*] when an intrusion is detected.

5.1.3. IDS data review (IDS_RDR)

Family Behaviour

This family defines the requirements for tools that should be available to authorised users to assist in the review of IDS System data.

Component levelling

IDS_RDR: IDS data review	1

IDS_RDR.1 IDS data review, provides the capability to read information from the System data and requires that there are no other users except those that have been identified as authorised users that can read the information.

Management: IDS_RDR.1

The following actions could be considered for the management functions in FMT:

a) maintenance (deletion, modification, addition) of the group of users with read access right to the System data.

Audit: IDS_RDR.1

The following actions should be auditable if IDS_RDR IDS data review is included in the PP/ST:

a) Basic: Reading of information from the System data.

b) Basic: Unsuccessful attempts to read information from the System data.

5.1.3.1. IDS_RDR.1 Restricted data review

Hierarchical to: No other components.

Dependencies: IDS_SDC.1 System data collection

IDS_RDR.1.1 The System shall provide [assignment: *authorised users*] with the capability to read [assignment: *list of System data*] from the System data.

IDS_RDR.1.2 The System shall provide the System data in a manner suitable for the user to interpret the information.

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

5.1.4. IDS data collection (IDS_SDC)

Family Behaviour

This family defines requirements for recording information from the targeted IT System resource(s).

Component levelling

IDS_SDC: IDS data collection	1

IDS_SDC.1 IDS data collection, defines the information to be collected from the targeted IT System resource(s), and specifies the data that shall be recorded in each record.

Management: IDS_SDC.1

There are no management activities foreseen.

Audit: IDS_SDC.1

There are no auditable events foreseen.

5.1.4.1. IDS_SDC.1 System data collection

Hierarchical to: No other components.

Dependencies: FPT_STM.1 Reliable time stamps

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

a) [selection: *Start-up and shutdown, identification and authentication events, data accesses, service requests, network traffic, security configuration changes, data introduction, detected malicious code, access control configuration, service configuration, authentication configuration., accountability policy configuration, detected known vulnerabilities*]; and

b) [assignment: *other specifically defined events*].

IDS_SDC.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

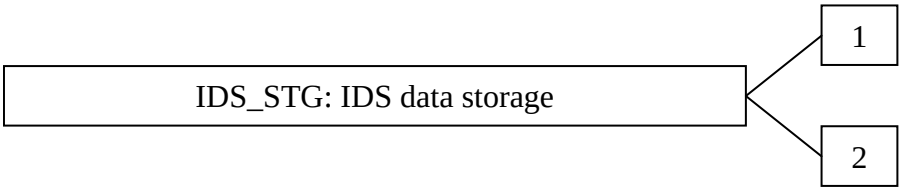
b) [assignment: *other additional information*].

5.1.5. IDS data storage (IDS_STG)

Family Behaviour

This family defines requirements for protecting IDS System data after it is recorded and stored by the TOE.

Component levelling



At IDS_STG.1 Guarantees of System data availability, specifies the guarantees that the TSF maintains over the system data given the occurrence of an undesired condition.

IDS_STG.2 Prevention of System data loss, specifies actions in case of exceeded storage capacity.

Management: IDS_STG.1

a) maintenance of the parameters that control the System data storage capability.

Management: IDS_STG.2

a) maintenance (deletion, modification, addition) of the actions to be taken in case of storage failure.

Audit: IDS_STG.1, IDS_STG.2

There are no auditable events foreseen.

5.1.5.1. IDS_STG.1 Guarantees of System data availability

Hierarchical to: No other components.

Dependencies: IDS_SDC.1 System data collection

IDS_STG.1.1 The System shall protect the stored System data from unauthorized deletion.

IDS_STG.1.2 The System shall protect the stored System data from modification.

IDS_STG.1.3 The System shall ensure that [assignment: *metric for saving System data*] System data will be maintained when the following conditions occur: [selection: *System data storage exhaustion, failure, attack*].

5.1.5.2. IDS_STG.2 Prevention of System data loss

Hierarchical to: No other components.

Dependencies: IDS_STG.1 Guarantees of system data availability

IDS_STG.2.1 The System shall [selection: '*ignore System data*', '*prevent System data, except those taken by the authorised user with special rights*', '*overwrite the oldest stored System data* '] and [assignment: *other actions to be taken in case of storage failure*] if the storage capacity has been reached.

6. Security Requirements

6.1. Definitions

6.1.1. Objects and Information

The TOE's primary purpose is to process information encoded in the form of IPv4 packets, flowing through the TOE. The TOE applies firewall, IDS/IPS, and VPN security functions on IPv4 packets. The user data objects that are used in the SFRs in this ST thus correspond to containers of network traffic information, i.e. IPv4 packets.

D.INFO Information flowing among internal and external networks, through the TOE. The information is generally associated with the security attributes of its container object, an IPv4 packet (D.PACKET).

D.PACKET A TOE representation of D.INFO, encoded in the form of an IPv4 packet. D.PACKET security attributes are described for FDP_IFF.1 /TFF.

6.1.2. Subjects

Subjects are defined in the CC as active entities in the TOE that perform operations on objects and information (passive entities in the TOE).

The subjects defined here are associated with user security attributes in the context of user-subject binding as specified in FIA_USB.1 /IFF and FIA_USB.1 /Admin.

S.VS A Virtual System is an active entity that performs firewall, IPS, and VPN-related operations in its own separate execution domain on a gateway, processing IPv4 packets (D.PACKET) and network information flows (D.INFO), reading and writing them from gateway interfaces.

S.MGMT The Security Management Server.

In order to improve readability, the SFRs presented in this ST identify users in place of subjects. For example, U.VPNPEER would represent a S.VS subject when bound to a particular VPN peer authorized external IT entity.

6.1.3. Users

Users are external entities that may attempt to bind to subjects in order to access TOE-protected assets. User security attributes are described for FIA_ATD.1.

U.USER An external IT entity that invokes TOE (S.VS) processing on an IPv4 packet (D.PACKET). A user is always identified by its presumed source address.

U.RAUSER A remote access VPN user is a special case of U.USER that establishes an authenticated trusted channel with the TOE (S.VS). In addition to the U.USER security attributes, a U.RAUSER is identified by a human user identifier authenticated in the course of trusted channel establishment and a VPN Security Association.

U.ADMIN	A human user that binds to the TOE (S.MGMT) in order to perform administrative operations.
U.AEITE	An authorized external IT entity as defined in the firewall PPs binds to the TOE, and after being successfully identified and authenticated is permitted to perform a limited number of security functions.
U.VPNPEER	A peer VPN gateway is a special case of U.AEITE that establishes an authenticated trusted channel with the TOE (S.VS) for sending and receiving information flows through the TOE. A U.VPNPEER is associated with a set of Security Associations and a VPN Domain.
U.OPSEC	A special case of an authorized external IT entity that binds to the TOE (S.MGMT) over a SIC-protected trusted path, in order to perform restricted administrative operations on TSF data using OPSEC client APIs (see section 1.5.3.14).

6.1.4. Security Function Policies

6.1.4.1. Unauthenticated SFP

Control of HTTP and SMTP traffic sent through the TOE is modeled using the [APP-PP] UNAUTHENTICATED SFP, enforced on information (D.INFO) passed through the TOE by external IT entities (U.USER) via unauthenticated application-level proxies (S.VS).

6.1.4.2. Authenticated SFP

The [APP-PP] AUTHENTICATED SFP controls FTP and Telnet traffic (D.INFO) sent through the TOE by authenticated users (U.USER or U.RAUSER) that initiate service and pass information via application-level proxies (S.VS).

6.1.4.3. Traffic Filter SFP

The TOE's traffic filter firewall security functionality is modeled using the TRAFFIC FILTER SFP, a refinement of the [TFF-PP] UNAUTHENTICATED SFP. The SFP controls flow of information (D.INFO) sent through the TOE by external IT entities (U.USER) bound to S.VS subjects.

The UNAUTHENTICATED SFP as defined in [TFF-PP] covers only unauthenticated information flows through the TOE. This information flow control SFP is generalized here to also cover authenticated information flows, so that this SFP is applied to all information flows through the TOE, whether authenticated or not.

6.1.4.4. VPN SFP

The TOE's VPN functionality is modeled using the VPN SFP. This SFP controls flow of information (D.INFO) sent and received over cryptographically-protected trusted

channels. The TOE (S.VS) applies decrypt-and-verify and encrypt-and-authenticate operations on incoming and outbound information, respectively, in accordance with the rules of this SFP.

6.2. 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 source for each requirement is denoted in column 3 of Table 6-1 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.

VIRT Requirement added to address virtualization objectives

VPN Requirement added to address VPN objectives[22].

FAUL Requirement added to address fault tolerance 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 6-1 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.

Table 6-1 –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_SAR.1	**Audit review**	**All**	**Refinement**	**Assignment**
FAU_SAR.2	**Restricted audit review**	**IDS**		**None**
FAU_SAR.3	**Selectable audit review**	**All**	**Refinement**	**Refinement**

[22] The SFRs added to this ST to address VPN objectives have not been drawn from any published VPN PP.

Functional Component		Source PP(s)	CC Operations Applied	
			Firewall PP	IDS PP
FAU_SEL.1	**Selective audit**	**IDS**		**Assignment**
FAU_STG.2	**Guarantees of audit data availability**	**All**	**Hierarchical, refinement**	**Refinement, assignment, selection**
FAU_STG.3	**Action in case of possible audit data loss**	**Other**	**Assignment**	
FAU_STG.4	**Prevention of audit data loss**	**All**	**Refinement**	**Refinement, selection**
FCS_CKM.1 /Asym	**Cryptographic key generation**	**DEP**	**Refinement, assignment**	
FCS_CKM.1 /Sym		**DEP**	**Refinement, assignment**	
FCS_CKM.2 /IKE	**Cryptographic key distribution**	**VPN**	**Refinement, assignment**	
FCS_CKM.2 /TLS		**Other**	**Refinement, assignment**	
FCS_CKM.4	**Cryptographic key destruction**	**DEP**	**Assignment**	
FCS_COP.1 /Admin	**Cryptographic operation**	**Both**	**None**	
FCS_COP.1 /TLS		**Other**	**Assignment**	
FCS_COP.1 /ESP		**VPN**	**Assignment**	
FCS_COP.1 /MAC		**VPN**	**Assignment**	
FCS_COP.1 /Hash		**Other**	**Assignment**	
FCS_COP.1 /Signature		**Other**	**Assignment**	
FCS_COP.1 /DH		**VPN**	**Assignment**	
FDP_ETC.2	**Export of user data with security attributes**	**VIRT**	**Assignment**	
FDP_IFC.1 /UNAUTH	**Subset information flow control**	**App**	**Refinement**	
FDP_IFC.1 /AUTH		**App**	**None**	
FDP_IFC.1 /TFF		**TFF**	**None**	
FDP_IFC.1 /VPN		**VPN**	**Assignment**	
FDP_IFC.2	**Complete information flow control**	**VIRT**	**Assignment**	

Functional Component		Source PP(s)	CC Operations Applied	
			Firewall PP	IDS PP
FDP_IFF.1 /UNAUTH	Simple security attributes	APP	Refinement, assignment	
FDP_IFF.1 /AUTH		APP	Refinement, assignment	
FDP_IFF.1 /TFF		TFF	Assignment	
FDP_IFF.1 /VPN		VPN	Assignment	
FDP_IFF.1 /VS		VIRT	Assignment	
FDP_ITC.2	Import of user data with security attributes	VIRT	Assignment	
FDP_RIP.2	Full residual information protection	Both	Hierarchical	
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, assignment
FIA_UAU.1	Timing of authentication	TFF, IDS	Refinement	Assignment
FIA_UAU.4	Single-use authentication mechanisms	TFF	None	
FIA_UAU.5	Multiple authentication mechanisms	APP	Refinement	
FIA_UID.2	User identification before any action	All	None	Hierarchical
FIA_USB.1 /IFF	User-Subject Binding	VIRT	Refinement, assignment	
FIA_USB.1 /Admin		Other	Assignment	
FMT_MOF.1	Management of security functions behavior	All	Refinement, Assignment	Refinement
FMT_MSA.1 /Attr	Management of security attributes	APP	Refinement	
FMT_MSA.1 /MAC		VIRT	Assignment	
FMT_MSA.1 /Rule		APP	Refinement	
FMT_MSA.1 /VPN		VPN	Assignment, selection	

Functional Component		Source PP(s)	CC Operations Applied	
			Firewall PP	IDS PP
FMT_MSA.3	**Static attribute initialization**	**Both, VPN, VIRT**	**Refinement**	
FMT_MTD.1	**Management of TSF data**	**APP, IDS**	**Refinement**	**Refinement, Assignment**
FMT_SMF.1	**Specification of Management Functions**	**DEP**	**Assignment**	
FMT_SMR.1	**Security roles**	**All**	**Refinement**	**Assignment**
FPT_FLS.1	**Failure with preservation of secure state**	**FAUL**	**Assignment**	
FPT_ITT.1	**Basic internal TSF data transfer protection**	**Other**	**Selection**	
FPT_STM.1	**Reliable time stamps**	**All**	**Refinement**	**Refinement**
FPT_TDC.1	**Inter-TSF basic TSF data consistency**	**DEP**	**Assignment**	
FPT_TRC.1	**Internal TSF consistency**	**FAUL**	**Assignment**	
FPT_TST.1	**TSF testing**	**FAUL**	**Selection, assignment**	
FRU_FLT.2	**Limited fault tolerance**	**FAUL**	**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**
IDS_RDR(EXP).1	**Restricted Data Review**	**IDS**		**Explicit, assignment refinement**

Functional Component		Source PP(s)	CC Operations Applied	
			Firewall PP	IDS PP
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**

6.2.1. Security Audit (FAU)

6.2.1.1. 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;

b) All auditable events for the not specified level of audit; and

c) the events in Table 6-2.

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 6-2.

Table 6-2 - Auditable Events

Functional Component	Auditable Event	Additional Audit Record Contents	Source PPs
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_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 configuration that occur while the audit collections functions are operating.		IDS
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_CKM.1	Success and failure of the activity	The object attribute(s), and object value(s) excluding any sensitive information.	DEP

Functional Component	Auditable Event	Additional Audit Record Contents	Source PPs
FCS_CKM.2	Success and failure of the activity.	The object attribute(s), and object value(s) excluding any sensitive information.	VPN, 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
FDP_ETC.2	All attempts to export information.		VIRT
FDP_IFF.1	All decisions on requests for information flow.	The presumed addresses of the source and destination subject.	Both
FDP_ITC.2	All attempts to import information.	Subject, object and information security attributes.	VIRT
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
FIA_UAU.1	Any use of the authentication mechanism.	The user identities provided to the TOE, location.	All
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).		VIRT, Other
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
FMT_MSA.3	Modifications of the default setting of permissive or restrictive rules. All modifications of the initial value of security attributes.		Other

Functional Component	Auditable Event	Additional Audit Record Contents	Source PPs
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_FLS.1	Failure of the TSF		FAUL
FPT_TDC.1	Used of the TSF data consistency mechanisms	Identification of which TSF data have been interpreted.	DEP
FPT_TRC.1	Restoring consistency upon reconnection.	Detected inconsistency between TSF data.	FAUL
FPT_TST.1	Execution of the TSF self tests and the results of the tests.		FAUL
FRU_FLT.2	Any failure detected by the TSF.		FAUL
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
IDS_ANL.1	Enabling and disabling of any of the analysis mechanisms.		Other
IDS_RCT.1	Actions taken due to detected intrusions.		Other
IDS_RDR.1	Reading of information from the System data; unsuccessful attempts to read information from the System data.		Other

6.2.1.2. User identity association (FAU_GEN.2)

FAU_GEN.2.1 For audit events resulting from actions of identified users, the TSF shall be able to associate each auditable event with the identity of the user that caused the event.

6.2.1.3. 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.

6.2.1.4. 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.

6.2.1.5. Selectable audit review (FAU_SAR.3)

FAU_SAR.3.1 The TSF shall provide the ability to apply **searches and sorting** of audit data based on**:**

a) user identity;

b) presumed subject address;

c) ranges of dates;

d) ranges of times;

e) ranges of addresses;

f) type of event; and

g) success or failure of related event.

6.2.1.6. 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;

b) **user identity**.

6.2.1.7. Guarantees of audit data availability (FAU_STG.2)

FAU_STG.2.1 The TSF shall protect the stored audit records **in the audit trail** from unauthorised deletion.

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

FAU_STG.2.3 The TSF shall ensure that **all**[23] **stored** audit records will be maintained when the following conditions occur: audit storage exhaustion, failure and/or attack.

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

FAU_STG.3.1 The TSF shall **send 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**.

6.2.1.9. 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.

[23] See the Table 7-1 FAU_STG.4 entry 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.

6.2.2. Cryptographic support (FCS)

6.2.2.1. Cryptographic key generation (FCS_CKM.1 /Asym)

FCS_CKM.1.1 The TSF shall generate **RSA and ECDSA** cryptographic keys in accordance with a specified cryptographic key generation algorithm **SP 800-90 Hash_DRBG (using SHA-256)** and specified cryptographic key sizes **1024, 2048 or 4096 binary digits in length for RSA, and 256, 384 or 521 binary digits in length for ECDSA** and that meet the following: **NIST SP 800-90, FIPS 186-2 and FIPS 140-2 (level 1)**.

6.2.2.2. Cryptographic key generation (FCS_CKM.1 /Sym)

FCS_CKM.1.1 The TSF shall generate **symmetric** cryptographic keys in accordance with a specified cryptographic key generation algorithm **SP 800-90 Hash_DRBG (using SHA-256)** and specified cryptographic key sizes **128-bit and 256-bit AES, 168-bit Triple DES** that meet the following: **NIST SP 800-90 and FIPS 140-2 (level 1)**.

6.2.2.3. Cryptographic key distribution (FCS_CKM.2 /IKE)

FCS_CKM.2.1 The TSF shall distribute cryptographic keys **for IPsec VPNs and authentication of external IT entities** in accordance with a specified cryptographic key distribution method **Internet Key Exchange (IKE)** that meets the following: **RFC 2409 (IKE) or RFC 5996 (IKEv2), with the following instantiation:**

a) For IKE Phase 1, the establishment of a secure authenticated channel between the TOE and another remote VPN endpoint shall be performed using either Main Mode or Aggressive Mode, as configured by an administrator;

b) The Diffie-Hellman key exchange[24] shall include groups 1, 2, and the groups 5 and 14 through 18 in accordance with RFC 3526 (768-, 1024-, 1536-, 2048-, 3072-, 4096-, 6144-, 8192-bit MODP, respectively), group 24 in accordance with RFC 5114 (2048-bit MODP with 256-bit Prime Order Subgroup), and groups 19 and 20 in accordance with RFC 5114 and RFC 4753 (256- and 384-bit Random ECP groups, respectively);

c) The pseudorandom function shall be the same as the negotiated hash algorithm in accordance with FCS_COP.1 /MAC;

d) The TSF shall be able to generate key material that provides perfect forward secrecy;

e) All random values used for IKE shall be randomly generated using a FIPS-approved random number generator in accordance with FCS_CKM.1 /Sym;

[24] 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). As defined in RFC 5996, IKEv2 performs the Diffie Hellman exchange in the first pair of messages (IKE_SA_INIT) and in a CREATE_CHILD_SA exchange when PFS is used.

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

- **Authentication with digital signatures: The TSF shall use RSA or ECDSA;**
- **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;**
- **Authentication with a pre-shared key: The TSF shall allow authentication using a pre-shared key; and**
- **The TSF also supports a Hybrid Mode[25] for remote access IPsec VPN where the gateway authenticates to the client with digital signatures and the human user is authenticated to the gateway with the support of the IT environment, in accordance with FIA_UAU.5.**

6.2.2.4. Cryptographic key distribution (FCS_CKM.2 /TLS)

FCS_CKM.2.1 The TSF shall distribute cryptographic keys **for SIC, SSL VPN and HTTPS Inspection** in accordance with a specified cryptographic key distribution method **TLS v1.0; and for SSL VPN and HTTPS Inspection, also: TLS v1.1 and TLS v1.2** that meets the following: **RFC 2246, RFC 4346, RFC 5246**.

6.2.2.5. Cryptographic key destruction (FCS_CKM.4)

FCS_CKM.4.1 The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method **overwriting** that meets the following: **FIPS 140-2 (level 1)**.

6.2.2.6. Cryptographic operation (FCS_COP.1 /Admin)

FCS_COP.1.1 The TSF shall perform encryption of remote authorized administrator sessions in accordance with a specified cryptographic algorithm: AES (Advanced Encryption Standard as specified in FIPS 197) encryption and cryptographic key sizes that are at least 128 binary digits in length that meet the following: FIPS PUB 140-2 (Level 1).

6.2.2.7. Cryptographic operation (FCS_COP.1 /TLS)

FCS_COP.1.1 The TSF shall perform **encryption and decryption of SSL VPN and HTTPS Inspection traffic** in accordance with a specified cryptographic algorithm: **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 140-2 (level 1); and (FIPS PUB 46-3 and NIST SP 800-67 for Triple DES; or FIPS PUB 197 and NIST SP 800-38A (CBC mode) for AES)**.

[25] Hybrid Mode is an extension to RFC 2409 defined in [HybridMode].

6.2.2.8. Cryptographic operation (FCS_COP.1 /ESP)

FCS_COP.1.1 The TSF shall perform **encryption and decryption of IPsec VPN traffic** in accordance with a specified cryptographic algorithm: **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: **RFC 2406 (Encapsulating Security Payload (ESP)); and (FIPS PUB 197 and NIST SP 800-38A (CBC mode) or NIST SP 800-38D (GCM mode) for AES or NIST SP 800-67 and FIPS PUB 46-3 with Keying Option 1 (K1, K2, K3 are independent keys) for Triple DES) and FIPS 140-2 (level 1)**.

6.2.2.9. Cryptographic operation (FCS_COP.1 /MAC)

FCS_COP.1.1 The TSF shall perform **production of Message Authentication Codes (MAC)** in accordance with a specified cryptographic algorithm: **HMAC-SHA-1; HMAC-SHA-256; or HMAC-SHA-384** and cryptographic key sizes **that are 160, 256, or 384 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 RFC 4868 (Using HMAC-SHA-256, HMAC-SHA-384, and HMAC-SHA-512 with IPsec) and FIPS 140-2 (level 1)**.

6.2.2.10. Cryptographic operation (FCS_COP.1 /Hash)

FCS_COP.1.1 The TSF shall perform **secure hash computation** in accordance with a specified cryptographic algorithm: **SHA-1; SHA-256; SHA-384; or SHA-512** and cryptographic key sizes **not applicable** that meet the following: **FIPS PUB 180-3 and FIPS 140-2 (level 1)**.

6.2.2.11. Cryptographic operation (FCS_COP.1 /Signature)

FCS_COP.1.1 The TSF shall perform **authentication with digital signatures** in accordance with a specified cryptographic algorithm: **RSA; or ECDSA** and cryptographic key sizes **1024, 2048 or 4096 binary digits in length for RSA, and 256, 384, and 521 binary digits in length for ECDSA** that meet the following: **PKCS #1, FIPS 186-2 and FIPS 140-2 (level 1)**.

6.2.2.12. Cryptographic operation (FCS_COP.1 /DH)

FCS_COP.1.1 The TSF shall perform **Key Agreement** in accordance with a specified cryptographic algorithm: **Diffie-Hellman** and cryptographic key sizes **768, 1024, 1536, 2048, 3072, 4096, 6144, 8192, 256 or 384 binary digits in length (for Diffie Hellman groups 1, 2, 5, 14 and 24, 15, 16, 17, 18, 19 or 20, respectively)** that meet the following: **RFC 2631, RFC 3526, RFC 5114, and RFC 4753**.

6.2.3. User data protection (FDP)

6.2.3.1. Export of user data with security attributes (FDP_ETC.2)

FDP_ETC.2.1 The TSF shall enforce the **MANDATORY ACCESS CONTROL SFP** when exporting user data, controlled under the SFP(s), outside of the TOE.

FDP_ETC.2.2 The TSF shall export the user data with the user data's **outbound logical interface's** associated **VLAN ID tag**.

FDP_ETC.2.3 The TSF shall ensure that the security attributes, when exported outside the TSC, are unambiguously associated with the exported user data.

FDP_ETC.2.4 The TSF shall enforce the following rules when user data is exported from the TSC: **no additional rules**.

Application Note: *The security attributes associated by the MAC Policy with user data are the attributes of the logical interface object to which the data is being written. These are uniquely associated with the interface's identity or VLAN ID (if defined). For VLAN interfaces, the TSF is required to correctly tag the exported data with the VLAN ID.*

6.2.3.2. Subset information flow control (FDP_IFC.1 /UNAUTH)

FDP_IFC.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**.

6.2.3.3. Subset information flow control (FDP_IFC.1 /AUTH)

FDP_IFC.1.1 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.

6.2.3.4. Subset information flow control (FDP_IFC.1 /TFF)

FDP_IFC.1.1 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: *According to the subject/object model described in [CC], an external IT entity is a user, not a subject, as a subject is defined as an active entity in the TOE. The external IT entity (U.USER or U.RAUSER or U.VPNPEER) binds to a TOE subject (S.VS), which performs operations on information (D.INFO) in the form of IPv4 packets (D.PACKET) on its behalf.*

The TRAFFIC FILTER SFP as defined covers all information flowing through the TOE. This includes information that is also controlled by the AUTHENTICATED and UNAUTHENTICATED SFPs, which relate to traffic that is mediated by protocol-specific application-level proxies. Note that the TOE applies the TRAFFIC FILTER SFP prior to the AUTHENTICATED or UNAUTHENTICATED SFPs.

6.2.3.5. Subset information flow control (FDP_IFC.1 /VPN)

FDP_IFC.1.1 TSF shall enforce the **VPN SFP** on**:**

a) subjects:

- **external IT entities (U.USER) that send and receive information through the TOE to one another (S.VS); and**
- **peer VPN entities (U.RAUSER, U.VPNPEER) bound to the TOE (S.VS);**

b) information: network traffic routed through the TOE (D.PACKET); and

c) operations:

- **pass information;**
- **encrypt and authenticate; or**
- **decrypt and verify**.

Application Note: *the VPN SFP as defined in this ST covers all information routed through the TOE. It supports three operations: pass information, encrypt and authenticate, and decrypt and verify. The first operation applies when no VPN rule matches the traffic; the other two operations refer to the sending and receiving, respectively, of information sent over a VPN tunnel established between the TOE and an authorized external IT entity.*

The two information flow control SFPs are enforced on the same types of subjects and information, meaning that both controls are applied to relevant traffic. See the rules in FDP_IFF.1 /VPN for the order in which these controls are applied and for their inter-dependencies.

6.2.3.6. Complete information flow control (FDP_IFC.2)

FDP_IFC.2.1 The TSF shall enforce the **MANDATORY ACCESS CONTROL SFP** on **information flowing through the TOE (D.INFO), subjects: Virtual Systems (S.VS),** and all operations that cause that information to flow to and from subjects covered by the SFP.

FDP_IFC.2.2 The TSF shall ensure that all operations that cause any information in the TOE to flow to and from any subject in the TOE are covered by an information flow control SFP.

Application Note: *The subjects covered by the Mandatory Access Control (MAC) Policy are the Virtual Systems (S.VS), which process user requests (network traffic).*

Users (U.USER) bind to S.VS subjects by sending information (D.INFO) to external TOE network interfaces, causing the corresponding subject to read information from the corresponding logical interface and to process it, in accordance with FDP_ITC.2.

Virtual Systems access the information in order to perform information flow control decisions (accept, drop, or reject), modify the information (e.g. for NAT), or otherwise manipulating the information (e.g. VPN encapsulation/decapsulation). Writing the information to a logical network interface exports information out of the TOE (optionally VLAN-tagged as described in FDP_ETC.2).

A Virtual System subject may transfer information to another Virtual System only if the two are associated with a common Virtual Router or Virtual Switch.

6.2.3.7. Simple security attributes (FDP_IFF.1 /UNAUTH)

FDP_IFF.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 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;
- 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 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**;

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.

6.2.3.8. Simple security attributes (FDP_IFF.1 /AUTH)

FDP_IFF.1.1 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 and user group memberships, established in accordance with FIA_USB.1** /Admin **and FIA_UAU.5**;

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 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
- 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:

- the human user initiating the information flow authenticates according to FIA_UAU.5;
- 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 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**;

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.

6.2.3.9. Simple security attributes (FDP_IFF.1 /TFF)

FDP_IFF.1.1 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;
- **user group memberships, if established in accordance with FIA_USB.1 /IFF and either FDP_IFF.1 /VPN or FDP_IFF.1 /AUTH;**

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 established in accordance with FDP_IFF.1 /VPN; and**
- **date and time of information flow event;**

c) additional stateful IP-based network packet attributes:

- **source service identifier; and**
- **for connection-oriented protocols:**
  - **sequence number;**
  - **acknowledgement number;**
  - **flags: SYN; ACK; RST; FIN**.

FDP_IFF.1.2 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) 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 **identified in FDP_IFF.1.1/TFF subsections a) and b)**, created by **an** authorized administrator;

b) the presumed address of the source subject, in the information, **is in the set of subject identifiers defined for either the logical interface on which traffic arrives or the VPN peer's VPN domain;**

c) the presumed address of the destination subject, in the information, translates to an address on the other connected network.

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

a) Fragmentation Rule: prior to applying the information policy ruleset, the TOE completely reassembles fragmented packets;

b) Stateful Packet Inspection Rule: the TSF tracks allowed established sessions and attempts to match received packets to sessions by matching the following packet attributes: source and destination addresses, source and destination service identifiers, and transport layer protocol. Connection-oriented protocol attributes defined in FDP_IFF.1.1/TFF subsection c) are also matched against the current session protocol state. The information flow policy ruleset, as defined in FDP_IFF.1.2/TFF, is applied to packets that do not match an allowed established session;

c) The TSF shall be capable of performing Network Address Translation (NAT) for presumed source and destination addresses and service identifiers in accordance with NAT rules configured by an authorized administrator;

d) The TRAFFIC FILTER SFP is applied prior to the UNAUTHENTICATED SFP or AUTHENTICATED SFP. Information flows denied or explicitly authorized by the TRAFFIC FILTER SFP are not processed by the UNAUTHENTICATED SFP or AUTHENTICATED SFP.

FDP_IFF.1.4 The TSF shall explicitly authorize an information flow based on the following rules:

a) Wire Mode: an authorized administrator may configure filtering exemptions for traffic that has been successfully decrypted and verified in accordance with FDP_IFF.1 /VPN with defined VPN community.

FDP_IFF.1.5 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 presumed address of the source subject is **not included in the defined set of subject identifiers.**

b) 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;

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** loopback **address.**

d) **The TOE shall reject requests in which the information received by the TOE contains the route (set of host network identifiers) by which information shall flow from the source subject to the destination subject**.

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.

Application Note: *The"service" attribute listed in FDP_IFF.1.1/TFF subsection b) is represented in the IP packet as a destination port number.*

Application Note: *The following notes, extracted from [PPFWTFMR], can provide useful guidance for the interpretation of the Fragmentation Rule and Stateful Packet Inspection Rule defined in FDP_IFF.1.3 subsections a) and b).*

This requirement has two distinctive rules that are applied. The first rule ensures that the TOE reassembles packets before applying the policy rules. The TOE ensures that fragments are handled properly and the TOE will drop any malformed packets (e.g., duplicate fragments, invalid offsets) and eliminates the security concern of fragments being received out of order at the target host.

The second rule, requires that the TOE maintains state for connection-oriented sessions and connectionless "pseudo" sessions. The TOE uses the stateful packet attributes to determine if a packet already belongs to a "session" that has been allowed by the TOE's ruleset. If a packet cannot be associated with a session, then the ruleset is applied. Connectionless sessions are subject to these rules and allow an IT entity to respond to a connectionless packet without having to specify a rule in the ruleset to explicitly allow the flow.

When a packet is received, usually "sanity" checks are made first (e.g., format and frame checks to make sure that the packet is well formed). If an address is all zeros (e.g., MAC address, Source IP address), the packet is discarded. If the packet passes the sanity checks, the TOE searches to see if the packet is associated with an existing session. If it is connectionless, the TOE may create a "pseudo session" to associate connectionless packets with a connection and therefore represent the connectionless data stream.

In an IP-based network stack, if a session already exists, the TCP packet's sequence number, acknowledgment number and flags (e.g., SYN, FIN) are checked to make sure that the packet really belongs to the session (e.g., an invalid sequence number can indicate a hijacked session). The ST author may include other security attributes (e.g., window size) if they so desire. If the checks pass, then the packet is allowed to pass. If the packet cannot be associated with an established session, the TOE's ruleset is applied to the packet.

Connection-less protocols (e.g., UDP) are included in the stateful inspection rules to allow for a "pseudo connection", which allows return traffic through the TOE without having to specify a rule in the TOE's ruleset.

6.2.3.10. Simple security attributes (FDP_IFF.1 /VPN)

FDP_IFF.1.1 The TSF shall enforce the **VPN SFP** based on the following types of subject and information security attributes:

a) subject (U.RAUSER, U.VPNPEER bound to S.VS) security attributes:

- **VPN community associations;**
- **Subject VPN domain;**
- **VPN domain for VPN peer;**
- **VPN Security Associations;**

b) information (D.PACKET) security attributes:

- **presumed source address;**
- **destination address;**
- **service;**
- **transport layer security attributes;**
- **VPN tunnel header**.

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

a) the TOE shall apply the operation decrypt and verify in accordance with FDP_UCT.1 and FDP_UIT.1 on inbound VPN-encapsulated information before enforcing the TRAFFIC FILTER SFP and where applicable, the UNAUTHENTICATED SFP or AUTHENTICATED SFP on the encapsulated information, if the information security attributes match a subject VPN security association established in accordance with FTP_ITC.1;

b) the TOE shall apply the operation encrypt and authenticate in accordance with FDP_UCT.1 and FDP_UIT.1 on outbound information flows that have been permitted by the TRAFFIC FILTER SFP and where applicable, the UNAUTHENTICATED SFP or AUTHENTICATED SFP if:

- **the destination address in the information is defined in the VPN domain of a VPN peer gateway belonging to an identified VPN community that also includes the subject; or**
- **the destination address in the information matches the client address of a subject remote access VPN security association established by the client in accordance with FTP_ITC.1;**

c) if neither of the above are applicable, the TOE shall permit the operation pass information if permitted by the TRAFFIC FILTER SFP.

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

a) Fragmentation Rule: prior to processing VPN-encapsulated information, the TOE completely reassembles fragmented packets;

b) Encrypt and Authenticate: for outgoing information whose destination address is defined in the VPN domain of a VPN peer gateway, belonging to an identified VPN community that also includes the subject, the TOE shall initiate the establishment of a VPN tunnel to the VPN peer in accordance with FTP_ITC.1;

c) VPN Community Association: the incoming or outgoing network traffic shall be associated with the identified VPN community, in the context of the enforcement of the TRAFFIC FILTER SFP.

FDP_IFF.1.4 The TSF shall explicitly authorize an information flow based on the following rules:

a) An authorized administrator may define a list of services (matching the service attribute in the information) excluded from VPN encapsulation.

FDP_IFF.1.5 The TSF shall explicitly deny an information flow based on the following rules:

a) The TOE shall reject plaintext (i.e. not VPN-encapsulated) requests for access or services where:

- **the presumed source address in the information is defined in the VPN domain of a VPN peer gateway, belonging to an identified VPN community that also includes the subject; and**
- **the destination address in the information is defined in the VPN domain of the subject;**

b) The TOE shall reject requests for access or services where the encrypt and authenticate operation applies, and a VPN tunnel cannot be established to the VPN peer;

c) The TOE shall reject requests for access or services where the decrypt and verify operation fails;

d) The TOE shall reject requests for access or services where the presumed source address in the VPN-encapsulated information, after a successful decrypt and verify operation, is not in the VPN domain of the VPN peer.

6.2.3.11. Simple security attributes (FDP_IFF.1 /VS)

FDP_IFF.1.1 The TSF shall enforce the **MANDATORY ACCESS CONTROL SFP** based on the following types of subject and information security attributes:

a) For Virtual System subjects (S.VS):

- **VSID;**
- **The set of logical interfaces and Warp links (connections to Virtual Routers and Virtual Switches) associated with the Virtual System; and**
- **Customer identifier;**

b) For information (D.INFO):

- **VSID**.

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

a) A Virtual System may access (read or modify) information only if the subject VSID equals the information VSID;

b) A Virtual System may transfer information to another Virtual System only if both are associated with a common Virtual Router or Virtual Switch;

c) A Virtual System may export information out of the TOE by writing it to a logical interface only if the logical interface is either directly associated with the Virtual System or is associated with a Virtual Router or Virtual Switch that is associated with the Virtual System.

FDP_IFF.1.3 The TSF shall enforce the **following additional information rules:**

a) If information is transferred from a source Virtual System to a target Virtual System in accordance with FDP_IFF.1.2 subsection b) above, The VSID of the information is set to the target Virtual System's VSID.

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

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

6.2.3.12. Import of user data with security attributes (FDP_ITC.2)

FDP_ITC.2.1 The TSF shall enforce the **MANDATORY ACCESS CONTROL SFP** when importing user data, controlled under the SFP, from outside of the TOE.

FDP_ITC.2.2 The TSF shall use the security attributes associated with the imported user data.

FDP_ITC.2.3 The TSF shall ensure that the protocol used provides for the unambiguous association between the security attributes and the user data received.

FDP_ITC.2.4 The TSF shall ensure that interpretation of the security attributes of the imported user data is as intended by the source of the user data.

FDP_ITC.2.5 The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TOE:

a) One of the following rules shall be applied to determine the logical interface associated with the imported information:

- **Imported data arriving on a physical interface for which VLAN tagging has not been defined (i.e. is defined with a single logical interface) shall be associated with the physical interface's defined logical interface;**
- **Untagged imported data arriving on a physical interface for which VLAN tagging has been defined shall be associated with the logical trunk interface for the physical interface;**
- **VLAN-tagged imported data will be associated with the logical interface associated with the data's VLAN ID tag; or**
- **Imported data whose VLAN tagging does not correspond to that of any of the logical interfaces defined for the physical interface on**

which traffic arrives shall be discarded and shall not be processed by the TSF.

b) The information shall be associated with the Virtual System ID (VSID) used to enforce the MANDATORY ACCESS CONTROL SFP as follows:

- **If the logical interface on which traffic arrives is directly associated with a Virtual System, the VSID for that VS; or**
- **If the logical interface on which traffic arrives is directly associated with a Virtual Router or Virtual Switch, the VSID of the Virtual System (connected to the Virtual Router or Virtual Switch) to which the traffic is routed by the Virtual Router or Virtual Switch; or**
- **Traffic arriving on a logical trunk interface shall be associated with VSID 0**.

6.2.3.13. 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[26].

Application Note: *FDP_RIP is a requirement derived from both firewall PPs. The 'objects' are defined as resources that are used by the subjects of the TOE to communicate through the TOE to other subjects, i.e. any buffers containing D.INFO or D.PACKETS.*

[TFF-PP] provides the following example for clarification of this requirement:

If, for example, the TOE pads information with bits in order to properly prepare the information before sending it out an interface, these bits would be considered a "resource". The intent of the requirement is that these bits shall not contain the remains of information that had previously passed through the TOE. The requirement is met by overwriting or clearing resources, (e.g. packets) before making them available for use.

6.2.3.14. Basic data exchange confidentiality (FDP_UCT.1)

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

6.2.3.15. Data exchange integrity (FDP_UIT.1)

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

[26] 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.

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

6.2.4. Identification and authentication (FIA)

6.2.4.1. 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;

c) authentication data; and

d) membership in user groups.

6.2.4.2. Timing of authentication (FIA_UAU.1)

FIA_UAU.1.1 The TSF shall allow **identification as stated in FIA_UID.2 and the following actions** on behalf of the user to be performed before the user is authenticated.

a) ICMP;

b) ARP;

c) IGMP;

d) Check Point RDP[27];

e) Download of the SSL Extender client from the TOE; and

f) the information flows specified by UNAUTHENTICATED SFP and TRAFFIC FILTER SFP.

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.

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.

IGMP queries and reports may optionally be enabled during TOE installation. This service is required in combination with certain networking devices for the use of ClusterXL multicast traffic.

[27] 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.

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.

6.2.4.3. Single-use authentication mechanisms (FIA_UAU.4)

FIA_UAU.4.1 The TSF shall prevent reuse of authentication data related to authentication attempts from either an internal or external network by:

a) authorized administrators;

b) authorized external IT entities.

Application Note: *See FIA_UAU.5 below for a specification of the single-use authentication mechanisms to be used by administrators and authorized external IT entities.*

6.2.4.4. Multiple authentication mechanisms (FIA_UAU.5)

FIA_UAU.5.1 The TSF shall provide single-use 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 or** single-use 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 or SIC certificate-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 certificate-based or IKE pre-shared secret or TLS certificate-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 an 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 or using single-use passwords (see below).

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.

IPsec/L2TP users may be authenticated using via TLS certificate-based authentication, or using single-use passwords (see below).

Where single-use 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].

6.2.4.5. 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.*

6.2.4.6. User-subject binding (FIA_USB.1 /IFF)

FIA_USB.1.1 The TSF shall associate the following security attributes **for a user sending information through the TOE** 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 the AUTHENTICATED SFP;

c) The group membership or memberships used to enforce the AUTHENTICATED and TRAFFIC FILTER SFPs;

d) The VSID used to enforce the MANDATORY ACCESS CONTROL SFP.

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 a user:

a) The subject acting on the behalf of the user is selected using the VSID associated with the information in accordance with FDP_ITC.2;

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

c) For users sending information over a IPsec VPN or SSL VPN Remote Access VPN tunnel, user identity is established from the identity transferred as part of the IKE or TLS protocols;

d) The identity for users establishing a IPsec/L2TP tunnel is established from the user identity transferred as part of the L2TP protocol. In addi-

tion, the client computer identity transferred as part of the IKE protocol is also associated with auditable events;

e) 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;

f) All user identities are associated with auditable events; and

g) Group memberships are associated with a subject acting on behalf of the user, established by 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 a user:

a) For users binding to the TOE over a VPN tunnel, the identity corresponding to the presumed source network identifier is changed to the tunneled presumed source network identifier; and

b) If the subject writes the information to another TOE Virtual System in accordance with the MANDATORY ACCESS CONTROL SFP[28], then:

- **The VSID associated with the information assumes the VSID of the other Virtual System; and**
- **If the presumed source address in the information has been modified by the TOE's NAT function, the associated user identity is changed to correspond to the modified traffic attributes**.

[28] i.e. the traffic is internally routed to another VS via a directly associated Warp interface or via a Virtual Router or Switch.

6.2.4.7. User-subject binding (FIA_USB.1 /Admin)

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

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

b) Administrator roles; and

c) Membership in user groups.

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) The user identity is associated with auditable events; and

c) Roles and group memberships are associated with a subject acting on behalf of the user, established by 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**.

6.2.5. Security Management (FMT)

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

FMT_MOF.1.1 The TSF shall restrict the ability to perform the functions **identified for FMT_MOF.1 in** Table 6-3 to an authorized administrator role as identified in Table 6-3.

6.2.5.2. Management of security attributes (FMT_MSA.1 /Attr)

FMT_MSA.1.1 The TSF shall enforce the UNAUTHENTICATED SFP**, AUTHENTICATED 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 **/UNAUTH, FDP_IFF.1.1 /AUTH, and FDP_IFF.1.1 /TFF, respectively** to the authorized administrator.

6.2.5.3. Management of security attributes (FMT_MSA.1 /MAC)

FMT_MSA.1.1 The TSF shall enforce the **MANDATORY ACCESS CONTROL SFP** to restrict the ability to query or modify the security attributes **Virtual System interface associations** to **the authorized administrator**.

6.2.5.4. Management of security attributes (FMT_MSA.1 /Rule)

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

6.2.5.5. Management of security attributes (FMT_MSA.1 /VPN)

FMT_MSA.1.1 The TSF shall enforce the **VPN SFP** to restrict the ability to create, query, modify and delete the security attributes **VPN rules described in FDP_IFF.1 /VPN** to **the authorized administrator**.

6.2.5.6. Static attribute initialization (FMT_MSA.3)

FMT_MSA.3.1 The TSF shall enforce the **MANDATORY ACCESS CONTROL SFP,** UNAUTHENTICATED SFP**, TRAFFIC FILTER SFP, VPN 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 Security Management server hosts, authentication protocols to any defined authorized authentication servers in the IT environment, as well as VPN-related protocols.

6.2.5.7. Management of TSF data (FMT_MTD.1)

FMT_MTD.1.1 The TSF shall restrict the ability to **operate on** the **TSF data identified for FMT_MTD.1 in Table 6-3** to **the roles identified in Table 6-3**.

6.2.5.8. 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 6-3 below.**

Table 6-3- Specification of Management Functions

Component	Management Function	Authorized Roles	Source PPs
FMT_MOF.1	start-up and shutdown	authorized administrator	TFF
	enable, disable the operation of the TOE	authorized administrator	APP
	create, delete, modify, and view default information flow security policy rules that permit or deny information flows	authorized administrator	TFF
	create, delete, modify, and view user attribute values defined in FIA_ATD.1	authorized administrator	TFF
	enable and disable single-use authentication mechanisms in FIA_UAU.4 and FIA_UAU.5	authorized administrator	Both
	control of communication with authorized external IT entities	authorized administrator	Both
	modify and set the time and date	no administrator role	TFF
	audit trail management	authorized administrator	APP
	archive, create, delete, and empty the audit trail	authorized	TFF

Component	Management Function	Authorized Roles	Source PPs
		administrator	
	review the audit trail	All roles in FMT_SMR.1	TFF
	backup of user attribute values, information flow security policy rules, and audit trail data, where the backup capability is supported by automated tools	authorized administrator	Both
	recover to the state following the last backup	authorized administrator	TFF
	enable and disable remote administration from internal and external networks	authorized administrator	TFF
	restrict addresses from which remote administration can be performed	authorized administrator	TFF
	modify the behaviour of the functions of System data collection, analysis and reaction	authorized administrator	IDS
	enabling SIC trust between Security Management and Security Gateway	authorized administrator	Other
FMT_MSA.1 /Attr	delete attributes from a rule, modify attributes in a rule, add attributes to a rule	authorized administrator	APP
FMT_MSA.1 /Rule	delete and create information flow rules described in FDP_IFF.1	authorized administrator	APP
FMT_MSA.1 /VPN	management of VPN rules	authorized administrator	VPN
FMT_MSA.1 /MAC	query, modify Virtual System interface and Customer associations	authorized administrator	VIRT
FMT_MSA.3	specification of alternative initial values to override the default values for Virtual System interface and Customer associations	authorized administrator	VIRT
	specification of default information flow security rules	authorized administrator	TFF
FMT_MTD.1	query, modify, delete, and assign the user attributes	authorized	APP

Component	Management Function	Authorized Roles	Source PPs
	defined in FIA_ATD.1.1	administrator	
	set the time and date used to form the timestamps in FPT_STM.1.1	no administrator role	APP
	query IDS System and audit data	All roles in FMT_SMR.1	IDS
	query and modify all other TOE data (other than IDS System and audit data)	authorized administrator	IDS
	management of the thresholds and actions taken in case of imminent audit storage failure	authorized administrator	Other

6.2.5.9. Security roles (FMT_SMR.1)

FMT_SMR.1.1 The TSF shall maintain the following roles: authorized administrator, authorized **audit** administrators.

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

6.2.6. Protection of the TSF (FPT)

6.2.6.1. Failure with preservation of secure state (FPT_FLS.1)

FPT_FLS.1.1 The TSF shall preserve a secure state when the following types of failures occur: **failure of a critical hardware or software entity**.

6.2.6.2. Basic internal TSF data transfer protection (FPT_ITT.1)

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

6.2.6.3. Reliable time stamps (FPT_STM.1)

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

6.2.6.4. Inter-TSF basic TSF data consistency (FPT_TDC.1)

FPT_TDC.1.1 The TSF shall provide the capability to consistently interpret **VLAN ID tags** when shared between the TSF and another trusted IT product.

FPT_TDC.1.2 The TSF shall use **[802.1q]** when interpreting the TSF data from another trusted IT product.

6.2.6.5. Internal TSF consistency (FPT_TRC.1)

FPT_TRC.1.1 The TSF shall ensure that TSF data is consistent when replicated between parts of the TOE.

FPT_TRC.1.2 When parts of the TOE containing replicated TSF data are disconnected, the TSF shall ensure the consistency of the replicated TSF data upon reconnection before processing any requests for **information flow**.

6.2.6.6. TSF testing (FPT_TST.1)

FPT_TST.1.1 The TSF shall run a suite of self tests during initial start-up and periodically during normal operation to demonstrate the correct operation of **the operational status of critical hardware and software entities**.

FPT_TST.1.2 The TSF shall provide authorised users with the capability to verify the integrity of **policy files**.

FPT_TST.1.3 The TSF shall provide authorised users with the capability to verify the integrity of stored TSF executable code.

6.2.7. Resource utilization (FRU)

6.2.7.1. Limited fault tolerance (FRU_FLT.2)

FRU_FLT.2.1 The TSF shall ensure the operation of all the TOE's capabilities when the following failures occur: **failure of a critical hardware or software entity**.

6.2.8. Trusted path/channels (FTP)

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

FTP_ITC.1.1	The TSF shall provide a communication channel between itself and another 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[29] or another 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**.

6.2.8.2. 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 and remote users to initiate communication via the trusted path.
FTP_TRP.1.3	The TSF shall require the use of the trusted path for **all access to the TOE by the authorized management roles identified in FMT_SMR.1**.

Application Note: *[CC] Part 2 distinguishes between local and remote users, as follows: Human users may further be differentiated as local human users, meaning they interact directly with the TOE via TOE devices (e.g. workstations), or remote human users, meaning they interact indirectly with the TOE through another IT product.*

In the context of the TOE, all administrators are local, in the sense that they are interacting directly with the TOE's Management GUIs, whereas users that are using non-TOE applications connecting to the TOE via OPSEC APIs (defined in FMT_SMR.1 as the OPSEC client role) are considered remote users.

[29] 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).

6.2.9. IDS Component Requirements (IDS)

6.2.9.1. 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:

a) signature; and

b) the TSF shall be able to maintain an internal representation of signature events and event sequences of known intrusion scenarios, encoded as IPS protections enabled by an authorized administrator, and to compare the signature events and event sequences against the record of system activity discernible from an examination of the network traffic mediated by the TOE; and

c) network protocol anomaly detection.

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; and

b) **No additional information**.

6.2.9.2. 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.

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

IDS_RDR(EXP).1.1 The System shall provide **all authorized management roles identified in FMT_SMR.1** with the capability to read **all 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.

6.2.9.4. 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; and

b) **no other specifically defined events**.

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 6-4.

Table 6-4 - 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**

6.2.9.5. 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.

6.2.9.6. 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 authorised user with special rights and send an alarm if the storage capacity has been reached.

6.3. 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.

No operations are applied to the assurance components.

Table 6-5- TOE Security Assurance Requirements

Assurance Class	Assurance Components	
Development	ADV_ARC.1	Security architecture description
	ADV_FSP.4	Complete functional specification
	ADV_IMP.1	Implementation representation of the TSF
	ADV_TDS.3	Basic modular design
Guidance Documents	AGD_OPE.1	Operational user guidance
	AGD_PRE.1	Preparative procedures
Lifecycle support	ALC_CMC.4	Production support, acceptance procedures and automation
	ALC_CMS.4	Problem tracking CM coverage
	ALC_DEL.1	Delivery procedures
	ALC_DVS.1	Identification of security measures
	ALC_FLR.3	Systematic flaw remediation
	ALC_LCD.1	Developer defined life-cycle model
	ALC_TAT.1	Well-defined development tools
Security Target evaluation	ASE_CCL.1	Conformance claims
	ASE_ECD.1	Extended components definition
	ASE_INT.1	ST introduction
	ASE_OBJ.2	Security objectives

Assurance Class	**Assurance Components**	
	ASE_REQ.2	Derived security requirements
	ASE_SPD.1	Security problem definition
	ASE_TSS.1	TOE summary specification
Tests	ATE_COV.2	Analysis of coverage
	ATE_DPT.1	Testing: basic design
	ATE_FUN.1	Functional testing
	ATE_IND.2	Independent testing – sample
Vulnerability Assessment	AVA_VAN.3	Focused vulnerability analysis

6.4. Security Requirements Rationale

6.4.1. Security Functional Requirements Rationale

Table 6-6 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 6-6 – 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.PROTCT	O.IDSENS	O.IDANLZ	O.RESPON	O.OFLOWS	O.INTEGR	O.MAC	O.VPN	O.FAULT
FAU_GEN.1							☑	☑	✓										
FAU_GEN.2								✓											
FAU_SAR.1							☑		◈										
FAU_SAR.2	×								◈										
FAU_SAR.3							☑		◈										
FAU_SEL.1							◈		◈										
FAU_STG.2	×			☑		☑			☑		◈				◈	◈			
FAU_STG.3															✓				
FAU_STG.4				☑		☑	◈		☑						◈				
FCS_CKM.1 /Asym		✓				✓												✓	
FCS_CKM.1 /Sym						✓												✓	
FCS_CKM.2 /IKE		✓																✓	
FCS_CKM.2 /TLS		✓				✓												✓	
FCS_CKM.4		✓				✓												✓	

	O.IDAUTH	O.SINUSE	O.MEDIAT	O.SECSTA	O.ENCRYP	O.SELPRO	O.AUDREC	O.ACCOUN	O.SECFUN	O.LIMEXT	O.PROTCT	O.IDSENS	O.IDANLZ	O.RESPON	O.OFLOWS	O.INTEGR	O.MAC	O.VPN	O.FAULT
FCS_COP.1 /Admin					☑														
FCS_COP.1 /TLS						✓												✓	
FCS_COP.1 /ESP																		✓	
FCS_COP.1 /MAC		✓																✓	
FCS_COP.1 /Hash		✓				✓												✓	
FCS_COP.1 /Signature		✓				✓												✓	
FCS_COP.1 /DH		✓																✓	
FDP_ETC.2																	✓		
FDP_IFC.1 /UNAUTH			☑																
FDP_IFC.1 /AUTH			☑																
FDP_IFC.1 /TFF			☑															✓	
FDP_IFC.1 /VPN																		✓	
FDP_IFC.2																	✓		
FDP_IFF.1 /UNAUTH			☑																
FDP_IFF.1 /AUTH			☑																
FDP_IFF.1 /TFF			☑															✓	
FDP_IFF.1 /VPN																		✓	
FDP_IFF.1 /VS																	✓		
FDP_ITC.2																	✓		
FDP_RIP.2			☑																
FDP_UCT.1																		✓	
FDP_UIT.1																		✓	
FIA_ATD.1	☑	☑							☑										
FIA_UAU.1	◈								◈										
FIA_UAU.4		☑																	
FIA_UAU.5	☑	☑																	
FIA_UID.2	☑							☑	◈										
FIA_USB.1 /Admin	✓							✓											

	O.IDAUTH	O.SINUSE	O.MEDIAT	O.SECSTA	O.ENCRYP	O.SELPRO	O.AUDREC	O.ACCOUN	O.SECFUN	O.LIMEXT	O.PROTCT	O.IDSENS	O.IDANLZ	O.RESPON	O.OFLOWS	O.INTEGR	O.MAC	O.VPN	O.FAULT
FIA_USB.1 /IFF	✓						✓	✓									✓		
FMT_MOF.1	×			☑					☑	☑	◈								
FMT_MSA.1 /Attr			☑	☑					☑										
FMT_MSA.1 /Rule			☑	☑					☑										
FMT_MSA.1 /VPN									✓									✓	
FMT_MSA.1 /MAC																	✓		
FMT_MSA.3			☑	☑					☑								✓		
FMT_MTD.1	×								☑		◈					◈			
FMT_SMF.1									✓	✓									
FMT_SMR.1	◈								☑										
FPT_FLS.1																			✓
FPT_ITT.1						✓													
FPT_STM.1							☑												
FPT_TDC.1			✓														✓		
FPT_TRC.1				✓															✓
FPT_TST.1				✓															✓
FRU_FLT.2																			✓
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									✓						◈				
ADV_ARC.1	×						×		×		×					×			

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 and data 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 /Admin and FIA_USB.1 /IFF determine 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.4 requires that single-use authentication mechanisms be used for authenticating administrators and authorized external IT entities.

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, single-use authenticators and/or a single-use password. FCS_CKM.2/TLS defines the authentication and key distribution protocol to be used for SIC and TLS-based user authentication, and FCS_CKM.2/IKE 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 /MAC defines the use of HMAC-SHA-1 as the keyed hash function;

- FCS_COP.1 /Hash defines the use of SHA-1 for secure hash computation;
- FCS_COP.1 /Signature defines the cryptographic algorithm used for authentication with digital signatures;
- FCS_COP.1 /DH defines the requirements for Diffie-Hellman key exchange.
- FCS_CKM.1 /Asym and FCS_CKM.4 define requirements for cryptographic key generation and destruction, respectively.

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/UNAUTH, FDP_IFC.1/AUTH and FDP_IFC.1 /TFF 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/UNAUTH, FDP_IFF.1/AUTH and FDP_IFF.1/TFF 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.

FPT_TDC.1 supports the definition of logical interfaces based on VLAN-tagging, used in the enforcement of the TRAFFIC FILTER SFP.

FMT_MSA.3 ensures that there is a default deny policy for the information flow control security rules. FMT_MSA.1/Attr and FMT_MSA.1/Rule 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/Attr and FMT_MSA.1/Rule 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 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. It 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_TST.1 requires that a suite of tests be run during initial start-up to verify the operational status of critical hardware and software entities, as well as verify the integrity of policy files and of stored TSF executable code.

FPT_TRC.1 requires that after a reconnection between parts of the TOE, the TSF shall ensure the consistency of the replicated TSF data before processing any requests for information flow.

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/Admin ensures that if the TOE does support authorized administrators to communicate with the TOE remotely from an internal or external network that AES 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.*

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.

FPT_ITT.1 was introduced to protect communication between distributed parts of the TOE (i.e. Security Management server to appliance management traffic). FTP_TRP.1 provides the administrator with a trusted path between the Management GUI and the Security Management server. FCS_CKM.2 /TLS, FCS_COP.1 /Admin and FCS_COP.1 /Hash support these requirements by providing key distribution, encryption and

decryption, and secure hash computation, respectively. FCS_CKM.1 /Asym and FCS_COP.1 /Signature define requirements for RSA key generation and signature in support of SIC authentication. FCS_CKM.1 /Sym provide key generation for symmetric keys. FCS_CKM.4 defines a requirement for secure key destruction. FMT_MOF.1 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 /Admin and FIA_USB.1 /IFF 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 6-3. FMT_MOF.1, and FMT_MSA.1/Attr and FMT_MSA.1/Rule , FMT_MSA.1/VPN and FMT_MTD.1 restrict

the use of these management functions to authorized administrator roles, as specified in Table 6-3.

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.

FMT_MOF.1 restricts management functions that can be used to modify the behavior of the communication with authorized external IT entities to the authorized administrator:

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

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. FMT_MOF.1 prevents unauthorized users from modifying IDS System data collection, analysis and reaction functions. FMT_MTD.1 provides the ability to restrict managing the behavior of functions of the TOE to authorized users of the TOE.

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.

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.

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 and anomaly-based intrusion analysis and generate conclusions, by matching network traffic mediated by the TOE against signature events and event sequences represented as INSPECT code fragments and regular expressions.

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 ensures that only authorized administrators may query or add audit and IDS System data.

O.MAC *The TOE must control access to resources in accordance with Virtual System domain separation rules based on the labeling of subjects and of the information being accessed.*

FDP_IFC.2 and FDP_IFF.1 /VS define the MANDATORY ACCESS CONTROL SFP including the security attributes of subject (Virtual Systems) and objects (interfaces) used to enforce the policy.

FIA_USB.1 /IFF determines the binding of a user sending information through the TOE with a subject, based on subject and information security attributes, in support of the enforcement of the MAC policy. FDP_ITC.2 and FDP_ETC.2, supported by FPT_TDC.1, allow the TOE to determine subject identity based on logical (VLAN-tagged) interfaces.

FMT_MSA.3 requires that restrictive default values are used for security attributes that are used to enforce the SFP, and that an authorized administrator may specify alternative initial values when an object or information is created.

FMT_MSA.1 /MAC allows authorized users to specify which resources may be accessed by which subjects.

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 /VPN and FDP_IFF.1 /VPN 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/VPN.

The following requirements define the cryptographic algorithms and protocols that must be used to meet this objective:

- FCS_CKM.2 /IKE requires the use of IKE cryptographic key distribution for IPsec VPNs;
- FCS_COP.1 /ESP requires support for Triple DES and AES for encryption and decryption of IPsec VPN traffic;
- FCS_CKM.2 /TLS requires the use of TLS cryptographic key distribution for SSL VPNs and for HTTPS Inspection;

- FCS_COP.1 /TLS requires support for Triple DES and AES for encryption and decryption of SSL VPN traffic;

FCS_COP.1 /MAC, FCS_COP.1 /Hash, FCS_COP.1 /Signature and FCS_COP.1 /DH define cryptographic algorithm requirements for production of Message Authentication Codes (MAC), secure hash computation, authentication with digital signatures and key agreement, respectively.

FCS_CKM.1 /Asym and FCS_CKM.1 /Sym define requirements for key generation. FCS_CKM.4 defines a requirement for secure key destruction.

O.FAULT *The TOE must be able to ensure that TOE security functions function correctly after a failure of a critical hardware or software entity.*

FPT_TST.1 defines a requirement for the TSF to test itself during initial start-up and periodically during normal operation to demonstrate the correct operation of critical hardware and software entities, as well as verifying the integrity of policy files and of stored TSF executable code. FPT_FLS.1 ensures that the TOE preserves a secure state when failures occur. FPT_TRC.1 supports this requirement by ensuring that TSF data is consistent when replicated between parts of the TOE, and that information flow requests are processed only after the TOE has ensured that it is in a consistent state.

FRU_FLT.2 ensures that the TOE's capabilities are fault tolerant.

6.4.2. 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. No operations are applied to assurance components.

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. This is desirable for a TOE designed to connect to public networks that do not necessarily operate under the same management control or security policy constraints as the TOE or its internal networks.

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.

6.4.3. Dependency Rationale

Table 6-7 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 6-7- Security Requirements Dependency Mapping

SFR	CC dependency	ST dependency	Dependency rationale
FAU_GEN.1	FPT_STM.1	FPT_STM.1	
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_SAR.1	FAU_GEN.1	FAU_GEN.1	
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	FAU_GEN.1, FMT_MTD.1	
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.1 /Asym	[FCS_CKM.2 or FCS_COP.1], FCS_CKM.4	FCS_COP.1 /Signature, FCS_COP.1 /DH, FCS_CKM.4	
FCS_CKM.1 /Sym		FCS_COP.1 /Admin**,** FCS_COP.1 /TLS**,** FCS_COP.1 /ESP, FCS_CKM.4	
FCS_CKM.2 /IKE	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1], FCS_CKM.4	FCS_CKM.1 /Asym, FCS_CKM.1 /Sym, FCS_CKM.4	
FCS_CKM.2 /TLS			
FCS_CKM.4	[FDP_ITC.1 or FDP_ITC.2 or	FCS_CKM.1 /Asym, FCS_CKM.1 /Sym	

SFR	CC dependency	ST dependency	Dependency rationale
	FCS_CKM.1]		
FCS_COP.1 /Admin	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1], FCS_CKM.4	FCS_CKM.1 /Asym, FCS_CKM.1 /Sym, FCS_CKM.4	
FCS_COP.1 /TLS			
FCS_COP.1 /ESP			
FCS_COP.1 /MAC			
FCS_COP.1 /Hash			
FCS_COP.1 /Signature			
FCS_COP.1 /DH			
FDP_ETC.2	[FDP_ACC.1 or FDP_IFC.1]	**FDP_IFC.2**	FDP_IFC.2 is hierarchical to FDP_IFC.1 so it can be used to satisfy the dependency.
FDP_IFC.1 /UNAUTH	FDP_IFF.1	FDP_IFF.1 /UNAUTH	
FDP_IFC.1 /AUTH		FDP_IFF.1 /AUTH	
FDP_IFC.1 /TFF		FDP_IFF.1 /TFF	
FDP_IFC.1 /VPN		FDP_IFF.1 /VPN	
FDP_IFC.2	FDP_IFF.1	FDP_IFF.1 /VS	
FDP_IFF.1 /UNAUTH	FDP_IFC.1, FMT_MSA.3	FDP_IFC.1 /UNAUTH, FMT_MSA.3	
FDP_IFF.1 /AUTH		FDP_IFC.1 /AUTH, FMT_MSA.3	
FDP_IFF.1 /TFF		FDP_IFC.1 /TFF, FMT_MSA.3	
FDP_IFF.1 /VPN		FDP_IFC.1 /VPN, FMT_MSA.3	
FDP_IFF.1 /VS		FDP_IFC.2, FMT_MSA.3	
FDP_ITC.2	[FDP_ACC.1 or FDP_IFC.1], [FTP_ITC.1 or FTP_TRP.1], FPT_TDC.1	**FDP_IFC.2**, FPT_TDC.1	FDP_IFC.2 is hierarchical to FDP_IFC.1 so it can be used to satisfy the dependency. The TOE does not provide a trusted channel for protection of the imported security attributes

SFR	CC dependency	ST dependency	Dependency rationale
			(VLAN tags). These are exchanged with the physically-connected bridge device, protected outside of the TOE in accordance with OE.VLAN.
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 /VPN	
FDP_UIT.1			
FIA_ATD.1	None		
FIA_UAU.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.
FIA_UAU.4			
FIA_UAU.5	None		
FIA_UID.2	None		
FIA_USB.1 /IFF	FIA_ATD.1	FIA_ATD.1	
FIA_USB.1 /Admin			
FMT_MOF.1	FMT_SMF.1, FMT_SMR.1	FMT_SMF.1, FMT_SMR.1	
FMT_MSA.1 /Attr	[FDP_ACC.1 or FDP_IFC.1], FMT_SMF.1, FMT_SMR.1	FDP_IFC.1 /UNAUTH, FDP_IFC.1 /TFF, FMT_SMF.1, FMT_SMR.1	
		FDP_IFC.1 /AUTH, FMT_SMF.1, FMT_SMR.1	
FMT_MSA.1 /MAC		**FDP_IFC.2**, FMT_SMF.1, FMT_SMR.1	FDP_IFC.2 is hierarchical to FDP_IFC.1 so it can be used to satisfy the dependency.
FMT_MSA.1 /Rule		FDP_IFC.1 /UNAUTH, FDP_IFC.1 /TFF, FMT_SMF.1, FMT_SMR.1	

SFR	CC dependency	ST dependency	Dependency rationale
		FDP_IFC.1 /AUTH, FMT_SMF.1, FMT_SMR.1	
FMT_MSA.1 /VPN		FDP_IFC.1 /VPN, FMT_SMF.1, FMT_SMR.1	
FMT_MSA.3	FMT_MSA.1, FMT_SMR.1	FMT_MSA.1 /Attr, FMT_MSA.1 /Rule, FMT_MSA.1 /VPN, FMT_MSA.1 /MAC, FMT_SMR.1	
FMT_MTD.1	FMT_SMF.1, FMT_SMR.1	FMT_SMF.1, FMT_SMR.1	
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.
FPT_FLS.1	None		
FPT_ITT.1	None		
FPT_STM.1	None		
FPT_TDC.1	None		
FPT_TRC.1	FPT_ITT.1	FPT_ITT.1	
FPT_TST.1	None		
FRU_FLT.2	FPT_FLS.1	FPT_FLS.1	
FTP_ITC.1	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		

SFR	CC dependency	ST dependency	Dependency rationale
IDS_STG(EXP).2	None		
ADV_ARC.1	ADV_FSP.1, ADV_TDS.1	**ADV_FSP.4, ADV_TDS.3**	Consistent with EAL4
ADV_FSP.4	ADV_TDS.1	**ADV_TDS.3**	Consistent with EAL4
ADV_IMP.1	ADV_TDS.3, ALC_TAT.1	ADV_TDS.3, ALC_TAT.1	
ADV_TDS.3	ADV_FSP.4	ADV_FSP.4	
AGD_OPE.1	ADV_FSP.1	**ADV_FSP.4**	Consistent with EAL4
AGD_PRE.1	None		
ALC_CMC.4	ALC_CMS.1, ALC_DVS.1, ALC_LCD.1	**ALC_CMS.4,** ALC_DVS.1, ALC_LCD.1	Consistent with EAL4
ALC_CMS.4	None		
ALC_DEL.1	None		
ALC_DVS.1	None		
ALC_FLR.3	None		
ALC_LCD.1	None		
ALC_TAT.1	ADV_IMP.1	ADV_IMP.1	
ATE_COV.2	ADV_FSP.2, ATE_FUN.1	**ADV_FSP.4,** ATE_FUN.1	Consistent with EAL4
ATE_DPT.1	ADV_ARC.1, ADV_TDS.2, ATE_FUN.1	ADV_ARC.1, **ADV_TDS.3**, ATE_FUN.1	Consistent with EAL4
ATE_FUN.1	ATE_COV.1	**ATE_COV.2**	Consistent with EAL4
ATE_IND.2	ADV_FSP.2, AGD_OPE.1, AGD_PRE.1, ATE_COV.1, ATE_FUN.1	**ADV_FSP.4,** AGD_OPE.1, AGD_PRE.1, **ATE_COV.2**, ATE_FUN.1	Consistent with EAL4
AVA_VAN.3	ADV_ARC.1, ADV_FSP.2, ADV_TDS.3, ADV_IMP.1, AGD_OPE.1, AGD_PRE.1	ADV_ARC.1, **ADV_FSP.4,** ADV_TDS.3, ADV_IMP.1, AGD_OPE.1, AGD_PRE.1	Consistent with EAL4

6.4.4. 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 6.2.2 therefore reference external standards that the implementation must meet when providing the required capabilities.

Table 6-8 summarizes the standards compliance claims made in Section 6.2.2 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 Security Gateway Appliances cryptographic algorithm certificates are referenced in [FIPSPOL].

Table 6-8- Cryptographic Standards and Method of Determining Compliance

Standard claimed	Cryptographic SFRs	Method of determining compliance
RFC 2409 (IKE), RFC 5996 (IKEv2)	FCS_CKM.2 /IKE	Vendor assertion
RFC 2406 (ESP)	FCS_COP.1 /ESP	
FIPS 140-2 Level 1	FCS_CKM.1, FCS_CKM.4, FCS_COP.1 (all iterations)	Cert. #1977
Hash_DRBG (SHA-256) as per NIST SP 800-90	FCS_CKM.1 /Asym, FCS_CKM.1 /Sym, FCS_CKM.2 /IKE	Cert. #199
Triple DES in CBC mode as per FIPS PUB 46-3	FCS_COP.1 /TLS, FCS_COP.1 /ESP	Cert. #1313 and #1314
AES in CBC mode as per FIPS PUB 197 and NIST SP 800-38A	FCS_COP.1 /Admin, FCS_COP.1 /TLS, FCS_COP.1 /ESP	Cert. #2037
AES in GCM mode as per FIPS PUB 197 and NIST SP 800-38D	FCS_COP.1 /ESP	Cert. pending
HMAC as per RFC 2104 and FIPS PUB 198	FCS_COP.1 /MAC	Cert. #1235 and #1236
SHA-1, SHA-256, SHA-384 and SHA-512 as per NIST PUB FIPS 180-3	FCS_COP.1 /Hash	Cert. #1782 and #1783
RSA digital signatures as per PKCS#1	FCS_COP.1 /Signature	Cert. #1057
ECDSA digital signatures as per	FCS_COP.1	Cert. pending

Standard claimed	**Cryptographic SFRs**	**Method of determining compliance**
FIPS 186-2	/Signature	
TLSv1.0 as per RFC 2246	FCS_CKM.2 /TLS	Vendor assertion
TLSv1.1 as per RFC 4346		
TLSv1.2 as per RFC 5246		
Diffie-Hellman as per RFC 2631, RFC 3526, and RFC 5114	FCS_COP.1 /DH	Vendor assertion

7. TOE Summary Specification

7.1. SFR Mapping

Table 7-1 provides a description of the general technical mechanisms that the TOE uses to satisfy each SFR defined in section 6.2. The table includes the description of security functionality given in each SFR by reference, and provides a high-level view of their implementation in the TOE, referencing section 1.5.1 and 1.5.3 for descriptions of the physical and logical components of the TOE, respectively.

See section 6.4.4 for the substantiation of the method used for determining compliance with cryptographic standards.

Table 7-1- TOE Summary Specification SFR Mapping

<table>
<tr><th>Component</th><th>Description of mechanism</th></tr>
<tr><td colspan="2">7.1.1. Security Audit (FAU)</td></tr>
<tr><td>FAU_GEN.1</td><td>Auditable events are identified by both Security Gateway and Security Management server management components.

Check Point Security Gateway Appliances can be configured to selectively generate audit records for matched security policy rules, including both packet inspection events and IPS events. VPN key exchange and encrypted packet handling events may also be logged.

Audit records are forwarded online to the Security Management server (in batches of every two seconds or 50 log records) for storage and for audit review. In a management high-availability configuration, the gateway can forward its log records to both active and standby Security Management servers. Backup log servers can also be configured in case connectivity is lost to the Security Management servers.

In a cluster configuration, Each gateway forwards its log records to independently; multiple records referring to a single connection are consolidated by the Security Management server.

The Security Management Server maintains a separate log file database for audit records related to administrator access and management operations.

Table 7-2 below, derived from Table 6-2, provides more details on how the TOE meets each auditable event requirement in FAU_GEN.1.

Table 7-2- Audit SF Mapping to FAU_GEN.1
<table>
<tr><th>Functional Component</th><th>Auditable Event</th><th>Mapping</th></tr>
<tr><td>FAU_GEN.1</td><td>Start-up and shutdown of audit functions</td><td>Audit functions start-up when a Security Gateway or Security Management server boots up, and cannot be disabled by an administrator.

Audit records are generated on start-up for both gateway and Security Management server host. Gateway shut-down can be identified by a log record generated by the Security Management server when</td></tr>
</table>
</td></tr>
</table>

Component	Description of mechanism		
			connectivity to the gateway is lost.
	FAU_GEN.1	Access to the IDS System	Management GUI logins are logged.
	FAU_GEN.1	Access to the TOE and System Data	Management GUI logins are logged. Object modifications are also logged, including the object ID and modified values.
	FAU_SAR.1	Reading of information from the audit records	Logins to the SmartView Tracker management GUI are audited.
	FAU_SAR.2	Unsuccessful attempts to read information from the audit records	Login failures to the SmartView Tracker management GUI are audited.
	FAU_SEL.1	All modifications to the audit configuration that occur while the audit collections functions are operating	Logging of audit configuration modifications.
	FAU_STG.3	Actions taken due to exceeding of a threshold	Logging of alert sent when a threshold is exceeded.
	FAU_STG.4	Actions taken due to the audit storage failure	Logging of alert sent when audit storage failure occurs.
	FCS_CKM.1	Success and failure of the activity.	Logging of SIC key generation, VPN key exchanges, and intra-TOE management sessions.
	FCS_CKM.2	Success and failure of the activity.	Logging of VPN key exchanges and intra-TOE management sessions.
	FCS_COP.1	Success and failure, and the type of cryptographic operation	Logging of VPN key exchanges, digital signature verification, encryption/decryption of network traffic and packet handling errors.
	FDP_ETC.2	All attempts to export information.	Logging of outbound Packet Inspection events.
	FDP_IFF.1	All decisions on requests for information flow.	Logging of Packet Inspection events.
	FDP_ITC.2	All attempts to import information.	Logging of incoming Packet Inspection events.
	FDP_UCT.1	All VPN security association establishments.	Logging of VPN key exchange events.
	FDP_UIT.1	All VPN security association establishments.	Logging of VPN key exchange events.
	FIA_UAU.1	Any use of the authentication mechanism.	Logging of successful and unsuccessful administrator logins,VPN tunnel establishment, and user authentication events. All log records include both presumed source address and user identity (for successful authentication events).
	FIA_UAU.5	The final decision on authentication.	
	FIA_UID.2	All use of the user	Administrator login events are logged,

Component	Description of mechanism		
		identification mechanism.	including the administrator's identity. Presumed source address identity is included in audit records generated for Packet Inspection-related auditable events. Audit records also include the user identities established as part of a remote access VPN secure channel establishment.
	FIA_USB.1	Success and failure of binding of user security attributes to a subject (e.g. success or failure to create a subject).	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, and logging of identity of VPN peer. Logging of successful and unsuccessful user authentication events.
	FMT_MOF.1	Use of the functions listed in this requirement pertaining to audit.	Logins to the SmartView Tracker management GUI are audited. An event record for an authorized System administrator accessing SmartView Tracker indicates log review, allowing the administrator to export the log records out of the TOE for backup or archiving purposes. Log switch and log purge operations are audited (in the new log file).
		All modifications in the behavior of the functions of the TSF	All security policy modifications are logged, as well as user account and certificate management, audit trail log-switches and purges. SIC trust establishment may be logged by establishing a logging rule for the SIC registration protocol.
	FMT_MSA.3	Modifications of the default setting of permissive or restrictive rules.	Logging of security policy modifications.
		All modifications of the initial value of security attributes.	Logging of security policy modifications.
	FMT_MTD.1	All modifications to the values of TSF data	Logging of security policy modifications, user management.
	FMT_SMF.1	Use of the management functions.	Administrator logins to the management GUIs are logged, as well as all Security Management database update operations.
	FMT_SMR.1	Modifications to the group of users that are part of the authorized administrator role.	Logging of user management operations.

Component	Description of mechanism		
		Unsuccessful attempts to authenticate the authorized administrator role.	Logging of unsuccessful attempts to log on as administrator.
	FPT_FLS.1	Failure of the TSF	The Security Management server generates a log record when a gateway becomes unreachable as a result of software, hardware, or network failures. Non-recoverable cluster member failures and cluster transitions are logged.
	FPT_TDC.1	Used of the TSF data consistency mechanisms	The logical interface is recorded for all logged incoming and outbound Packet Inspection events. The logical interface uniquely identifies a VLAN ID tag, as defined by the authorized System administrator.
	FPT_TRC.1	Restoring consistency upon reconnection.	Logging of Full Synchronization sessions and retrieval of updated security policy from the Security Management server.
	FPT_TST.1	Execution of the TSF self tests and the results of the tests.	The Management GUIs display Security Gateway and Security Management host operational status, as well as policy installation status. Thresholds can be set to generate alerts when a failure occurs.
	FRU_FLT.2	Any failure detected by the TSF.	
	FTP_ITC.1	All attempted uses of the trusted channel functions.	Logging of VPN key exchange events and encryption/decryption of network traffic.
	FTP_TRP.1	All attempted uses of the trusted path functions	Logging of administrator logins to the management GUIs.
	IDS_ANL.1	Enabling and disabling of any of the analysis mechanisms.	Logging of security policy modifications.
	IDS_RCT.1	Actions taken due to detected intrusions.	Each Alert generation automatically causes a corresponding log record to be recorded. An authorized administrator can selectively configure logging for each IDS/IPS event.
	IDS_RDR.1	Reading of information from the System data. Unsuccessful attempts to read information from the System data.	Logging of administrator logins, successful and unsuccessful, to the SmartView Tracker management GUI.
FAU_GEN.2	All audit records generated in accordance with FAU_GEN.1 contain user identification, except where there is no identified user, e.g. for audit records generated for system start-up and shutdown. Packet inspection event records always include the presumed source address and logical interface on which the traffic was received. Remote access VPN audit records include the authenticated user identity. When IPsec/L2TP is used for remote access VPN, the audit records also include the authenticated client computer identity. Audit records generated for administrator actions include the administrator account identification.		
FAU_SAR.1	Authorized administrators and authorized audit administrators use the SmartView Tracker		

Component	Description of mechanism
	Management GUI to review audit trail data. SmartView Tracker provides both tabular and form-based human-readable representations of the audit records, and allows the administrator to perform searches and sorting and configure various views that aid in interpreting the information. OPSEC clients access audit records via non-TOE applications using the LEA OPSEC API (see section 1.5.3.14). LEA is a well-defined API that provides log record information, including a data dictionary that assists the application in interpreting the information.
FAU_SAR.2	The Security Management Server installation is protected from any external access by a Security Gateway, as described in section 1.5.1.5. Once the TOE is operational, all access to the installation is performed using the management GUIs or using OPSEC APIs. Each such access request is authenticated using the SIC facility. Security Management determines the authorisations of the identified user; only users defined as having log review privileges can view the contents of the audit log database.
FAU_SAR.3	SmartView Tracker allows the administrator to 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 Security Gateway 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. 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 TOE 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 security policy installed on the Security Gateway by the authorized administrator determines which Packet Inspection, IPS, and VPN events generate audit records, based on event type. The policy can also be configured to inhibit log generation for a set of presumed source addresses, or authenticated user identity, by setting up no-Log rules that match relevant network traffic.
FAU_STG.2, FAU_STG.3, FAU_STG.4	Audit records are stored in a log database on the Security Management server installation, protected from any external access by a Security Gateway. Once the TOE is operational, all access to the installation is performed using the management GUIs or using OPSEC APIs. Access to log records is performed using the SmartView Tracker management GUI application, or via the LEA API. Security Management authenticates both management GUI and OPSEC API users, providing a SIC trusted path for all management operations. A SmartView Tracker user must have Read/Write *Track Logs* and *Audit Logs* privileges in order to delete audit records associated with gateway events or Security Management events, respectively. There is no interface allowing

Component	Description of mechanism
	modification of audit records. The LEA API provides only read-only access to audit records. Security Gateways maintain a queue of log records generated on the gateway in memory, while they are being transmitted over the network to the defined log servers. If this queue is overrun, i.e. if the gateway consistently generates log records faster than they can be received by the log server, or if there is a connectivity failure to the log server, the gateway stores the queued records in local log files, so that no log records are lost. In the event of failure, e.g. loss of power on the gateway, queued audit records that have not been successfully transmitted to the log server may be lost. The maximum number of records that may be lost is equal to the queue size: 4096 records. When disk space on the Security Management host falls below a predefined threshold, the server stops collecting audit records. As explained above, gateways will queue the records, and eventually start logging them to the local disk, until connectivity is resumed (i.e. until the administrator frees up storage on the Security Management host or redirects the gateway to log to another log server). If the disk space on the gateway falls below another predefined threshold, the gateway 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 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, administrators can monitor disk, memory and CPU resources on both gateways and Security Management server hosts. 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.
7.1.2. Cryptographic support (FCS)	
FCS_CKM.1 /Asym	RSA keys are generated by the TOE in support of IPsec VPN (IKE), SSL VPN, SIC, and HTTPS Inspection functionality. The TOE supports RSA key generation with key lengths of 1024, 2048 and 4096 bits. The TOE can also generate ECDSA keys for IKE, with key lengths of 256, 384 and 521 bits. RSA and ECDSA key generation uses the underlying FIPS 140-2 compliant SP 800-90 DRBG described below for FCS_CKM.1 /Sym. SIC keys are generated by the ICA, described in section 1.5.3.13 (see also below for FCS_CKM.2 /TLS). Security Gateway keys (and certificates) are securely delivered to the gateway as part of SIC trust establishment. Administrator keys (and certificates) are distributed manually on removable media. Security Gateway VPN keys are generated by the Security Management Server. The private key and certificate (generated with the support of an external certificate authority in the IT environment) are included in the security policy delivered from the Security Management Server to the Security Gateway. Note: The ICA can also generate VPN certificates for RSA private keys. However, the evaluated configuration does not allow external access to the Security Management server, thereby preventing access to ICA CRLs. Therefore, an external certificate authority in the IT environment must be used to manage VPN certificates for the TOE and its VPN peers.
FCS_CKM.1 /Sym	Symmetric keys are generated using a FIPS 140-2 compliant SP 800-90 Hash_DRBG algorithm, implemented using SHA-256 as the hash function. The TOE gathers entropy for the DRBG into an entropy pool from various sources, including

Component	Description of mechanism
	operating system supplied entropy (/dev/urandom), a high precision timer, process status, memory usage, network events, and I/O status. In addition, an administrator may choose to provide additional entropy during TOE installation through keyboard input timing. The entropy pool is used to seed and periodically reseed the DRBG.
FCS_CKM.2 /IKE, FCS_COP.1 /ESP, FCS_COP.1 /MAC, FCS_COP.1 /Hash, FCS_COP.1 /Signature, FCS_COP.1 /DH	Gateway VPN daemons maintain a set of active Security Associations for IKE, IPsec, SSL VPN (TLS) and HTTPS Inspection sessions. Either the TOE or a Peer VPN gateway may initiate key exchange over the IKE protocol for site-to-site VPN. Remote access VPN is always initiated by the client, for both IKE/IPsec and for TLS-based VPN. Both IKE ([RFC2409]) and IKEv2 ([RFC5996]) are supported. IKE phase 1 is supported using either Main Mode (default) or Aggressive Mode. The TOE supports Diffie-Hellman groups[30] 1, 2, 5, 14 through 20, and 24. The pseudo random function used in IKE is the same as the negotiated hash algorithm; HMAC-SHA-1, HMAC-SHA-256 or HMAC-SHA-384 are supported. Gateway authentication can be configured to use either RSA or ECDSA digital signatures, or pre-shared secrets. Client authentication can be configured to use either RSA digital signatures, or a user password, authenticated to the gateway in accordance with [HybridMode]. In the latter case, the gateway sends the user's presumed identity and password to an authentication server in the IT environment in order to authenticate the user. TOE evaluated configuration guidance requires that only single-use password mechanisms be used. Where digital signature authentication is used, the gateway performs X.509v3 certificate path validation, and as configured by an administrator, checks for certificate revocation using the LDAP, HTTP, or OCSP protocols. The TOE supports PKCS#1 encoded RSA key lengths of 1024, 2048, and 4096 bits, and ECDSA keys using EC curves P-256, P-384 and P-521, as defined in FIPS 186-2. SHA-1, SHA-256, SHA-384 and SHA-512 are supported as certificate integrity algorithms. The TOE supports IKE [ConfigMode] and IKEv2 Configuration Payload (CP) for allocating an *Office Mode* IP address to a remote access IPsec VPN client, to be used in IKE Phase II and within IPsec ESP-encapsulated packets. IKE Phase II is performed using Quick Mode, with perfect forward secrecy (PFS) supported as an option. PFS is supported with IKEv2 as well. IPsec ESP is performed in tunnel mode in accordance with [RFC2406], providing data confidentiality and integrity protection. ESP transport mode can also be supported when requested by a VPN peer (the TOE always initiates tunnel mode). The TOE can be configured to support either 128 or 256 bit AES or Triple DES in CBC mode for confidentiality protection. The negotiated hash algorithm as described above is used as the algorithm for producing message authentication codes. The TOE also supports AES in GCM mode, which provides both confidentiality and integrity protection. IKE negotiations can be performed over either UDP or TCP. NAT traversal (NAT-T) is supported for both IKE and IPsec, in accordance with [RFC3947] and [RFC3948], respectively, and for IKEv2 in accordance with [RFC5996]. In addition, the TOE supports a proprietary TCP-based *Visitor Mode* tunneling protocol that allows remote access VPN clients to tunnel IKE, IKEv2 and ESP over a single TCP port (e.g. 443).
FCS_CKM.2 /TLS, FCS_COP.1 /Admin,	The TOE supports the TLSv1.0 secure channel protocol, in accordance with [RFC2246]. It also supports TLSv1.1 in accordance with [RFC4346] and TLSv1.2 in accordance with [RFC5246]. TLSv1.0 is used for four purposes: remote access SSL VPN, Secure Internal Communications (SIC) between TOE components, HTTPS Inspection and for IPS Update downloads. The TLSv1.1 and TLSv1.2 protocols are also supported for SSL VPN and HTTPS Inspection. The

[30] The TOE supports additional Diffie-Hellman groups which are not included in the evaluation.

Component	Description of mechanism
FCS_COP.1 /TLS, FCS_COP.1 /Hash, FCS_COP.1 /Signature	specific protocol version used is negotiated with the TLS client (the authorized administrator may configure the set of supported protocol versions). The ciphersuite used for SSL VPN is TLS_RSA_WITH_3DES_EDE_CBC_SHA. For SIC communications, the ciphersuite used is TLS_RSA_WITH_AES_128_CBC_SHA. IPS updates are downloaded over a TLS session established with the TLS_DHE_RSA_WITH_AES_256_CBC_SHA ciphersuite. Gateways support remote access SSL VPN by allowing a remote user to connect to a Security Gateway over a Visitor Mode tunnel, establishing a TLSv1.0 session with the gateway. The same digital signature and password-based authentication mechanisms used for IPsec VPN are used for TLS client and gateway authentication. The Security Management server contains an internal certificate authority (ICA) as described in section 1.5.3.13. The ICA generates X.509v3 certificates that are used for internal communications between the server and managed virtual entities, as well as with external clients using OPSEC APIs. SHA-1, SHA-256, SHA-384 and SHA-512 are supported as certificate integrity algorithms. The ICA supports PKCS#1 encoded RSA, with key lengths of 1024, 2048 and 4096 bits. CRLs are distributed to TOE components as part of the SIC session establishment for management protocols. TOE components always use ICA-issued certificates for establishing SIC TLS sessions. Administrators may authenticate using ICA certificates, or by providing a password that is authenticated with the support of an authentication server in the IT environment. Where client certificates are used for authentication, TLS client authentication is used, providing mutual authentication as part of TLS session establishment. When passwords are used, TLS session establishment authenticates the server to the client; the client then sends the user's password to the server for authentication with the support of the IT environment.
FCS_CKM.4	All buffers containing cryptographic keying material are overwritten with zeros before being deallocated, so that previous contents are made unavailable when allocating the buffer for any object. Persistent and cached keys are stored on disk, and may be overwritten by the administrator by performing a product reinstallation. The installation process reformats all hard drives on both Security Management Server hosts and Security Gateways.

7.1.3. User data protection (FDP)

FDP_IFC.2, FDP_IFF.1 /VS	By default, the gateway is defiend with a single VRF, with VSID 0. The authorized administrator can define Virtual System, Virtual Router, and Virtual Switch entities and associate gateway logical interfaces with these virtual entities. When an IPv4 packet is received by the gateway, it is labeled with a VSID in accordance with FDP_ITC.2, and dispatched for processing by the corresponding Virtual System in accordance with FIA_USB.1 /IFF. Each VS maintains its own VRF tables, in which only its associated (physical, logical, and Warp) interfaces are registered. Each VS is allocated an independent set of processes for information flow processing in the context of the Virtual System's VRF. Packet Inspection can result in either blocking the packet, or passing it through (modified or unmodified). Packets can either be written to a directly associated interface, or handed over a Warp interface to a Virtual Router or Virtual Switch, and hence forwarded to an interface associated with that virtual entity.
FDP_ETC.2	The TOE supports VLAN tagging in accordance with [802.1q], for both incoming and outgoing traffic. The TOE uses VLAN ID tags to map the packet to a defined logical interface.
FDP_IFC.1	Information flow mediation is described in section 1.5.3.2 and 1.5.3.3.

Component	Description of mechanism
/TFF FDP_IFF.1 /TFF	Every IPv4 packet received by the Check Point Security Gateway Appliances gateway is intercepted by the firewall kernel. Fragmented packets are first reassembled. IPv4 packets with unauthorized IP options (e.g. source route option) are dropped. The logical interface over which the packet was received determines the VSID, in accordance with FDP_ITC.2. The packet is dispatched for processing by the corresponding Virtual System, determining the selection of the state tables and security policy that will be used to process the packet. 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 as a spoofed packet. Note that broadcast and loopback addresses are never considered valid source addresses and are therefore rejected. ESP-encapsulated packets are first decrypted and verified as described below for FDP_IFF.1 /VPN. If this is successful, the decapsulated packet contents are labeled with the VPN community on which the packet was received. If Wire Mode has been configured for this community and for the individual gateway, the packet is forwarded onward without further packet inspection. The packet header attributes are used to match the packet against state tables that contain accepted 'connections'. If the packet is successfully matched and passes packet sanity checks (correct sequence number, acknowledgment number, flags, etc. – see also application notes for FDP_IFF.1 /TFF), then it is concluded that a decision has been already made for this traffic flow, and processing may skip to Post-Inspect. A Virtual Machine (VM) now matches the packet against rules encoded in a machine language-like declarative language named 'INSPECT' (see also below, for IDS_ANL(EXP).1). 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, modifying addresses (i.e. NAT), and generating log messages. Packet Inspection is also applied on all packets outbound from the gateway.
FDP_IFC.1 /VPN, FDP_IFF.1 /VPN	VPN functionality is described in section 1.5.3.5. As described above for FDP_IFF.1 /TFF, ESP-encapsulated packets are processed in the gateway's operating system kernel before the VM rule base is applied to the packet. ESP packet fragments are reassembled before they processed further. If the packet matches an existing Security Association in the Security Gateway's state tables, it is decrypted and verified. The gateway verifies that the encapsulated packet's presumed address is within the VPN peer's VPN domain, before the encapsulated IP packet undergoes Packet Inspection. Packets that fail verification checks are dropped. In addition, the VPN kernel matches every non-ESP packet against VPN community definitions. If the packet **should** have been encrypted but was not, it is dropped. An authorized System administrator may define a list of services that are excluded from VPN encapsulation. Outbound packets are also matched against VPN community rules, after they are passed through by Packet Inspection. If the security policy requires that the packet be encrypted, the VPN kernel applies the cryptographic functions in the relevant Security Association (SA). If an SA cannot be

<table>
<tr><th>Component</th><th>Description of mechanism</th></tr>
<tr><td></td><td>found for a site-to-site VPN, the gateway puts the packet in a temporary hold state and attempts to negotiate a Security Association with the VPN peer, using the IKE protocol as described above for FCS_CKM.2 /IKE.

Visitor Mode and SSL VPN traffic is tunneled over TCP. The VPN daemon terminates the TCP session, extracts the tunneled packets, and injects them back into the kernel. Outbound traffic is transmitted through the daemon and back to the client over the established tunnel.</td></tr>
<tr><td>FDP_IFC.1 /UNAUTH, FDP_IFF.1 /UNAUTH, FDP_IFC.1 /AUTH, FDP_IFF.1 /AUTH</td><td>Security Servers are proxy processes that can be run on the Security Gateway 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 by tracking protocol state and matching mediated protocol request and response messages against expected messages for the current state. In addition, the following content security protection functionality is provided for each supported protocol:
<table>
<tr><th>Protocol</th><th>Protection</th><th>Description</th></tr>
<tr><td>FTP</td><td>FTP Commands</td><td>Allows only an administrator-defined 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.</td></tr>
<tr><td></td><td>Known Ports and Port Overflow</td><td>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.</td></tr>
<tr><td></td><td>Resource controls</td><td>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.</td></tr>
<tr><td>Telnet</td><td>Option control</td><td>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.</td></tr>
<tr><td>HTTP</td><td>Directory Traversal</td><td>Checks URL for an illegal combination of directory traversal characters.</td></tr>
<tr><td></td><td>Malicious HTTP Encodings</td><td>Blocks NULL encodings in URIs.</td></tr>
<tr><td></td><td>Non Compliant HTTP</td><td>Allows the authorized administrator to block various non-compliant protocol messages, including malformed separators, incorrectly specified whitespace characters, duplicate header values, deviation from chunked body format, recursive URL encoding, and empty value headers.</td></tr>
<tr><td></td><td>HTTP Format Sizes</td><td>Allows the authorized administrator to constrain the maximum URL length, maximum header lengths, request body length, and the number of headers.</td></tr>
<tr><td></td><td>ASCII Only Request</td><td>Blocks request headers or form fields with non-ASCII characters.</td></tr>
<tr><td></td><td>ASCII Only Response</td><td>Blocks response headers with non-ASCII characters.</td></tr>
</table></td></tr>
</table>

<table>
<tr><th>Component</th><th>Description of mechanism</th></tr>
<tr><td></td><td>
<table>
<tr><td></td><td>Headers</td><td></td></tr>
<tr><td></td><td>Header Rejection</td><td>Allows the authorized administrator to define header names or header name/value pairs that will be blocked in HTTP requests and responses.</td></tr>
<tr><td></td><td>HTTP Methods</td><td>Block HTTP requests with an administrator-defined HTTP method (e.g. GET and POST), URL, or scheme.</td></tr>
<tr><td>SMTP</td><td>Mail and Recipient Content</td><td>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.</td></tr>
<tr><td></td><td>Resource control</td><td>An authorized administrator can configure restrictions for attachment types and mail size.</td></tr>
</table>
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).
</td></tr>
<tr><td>FDP_ITC.2</td><td>The TOE supports VLAN tagging in accordance with [802.1q], for both incoming and outgoing traffic. The operating system on gateways uses VLAN ID tags to map the packet to a defined logical network interface object, in accordance with the rules described in FDP_ITC.2.

The TOE maintains the set of associations between virtual entities and logical network entities. These are used for associating the information received on a given logical interface with a VSID, in support of user-subject binding as described for FIA_USB.1 /IFF.

Before being explicitly associated with a virtual entity by an authorized System administrator, logical interfaces are implicitly associated with a Virtual System identified as VSID 0, which also handles all trunk traffic on all VLAN-tagged network interfaces. For each gateway, Virtual System VSID 0 is modeled in the management GUI applications as corresponding to the gateway object itself.</td></tr>
<tr><td>FDP_RIP.2</td><td>When an incoming network frame is received by a Check Point Security Gateway Appliances gateway, 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. This ensures that residual information that might remain from another packet is not retained.

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.</td></tr>
<tr><td>FDP_UCT.1</td><td>IPsec and TLS provide transmitted and received objects with protection from unauthorized disclosure. It also protects the data from modification, deletion, insertion and replay conditions,</td></tr>
</table>

Component	Description of mechanism
FDP_UIT.1	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.

7.1.4. User identification and authentication (FIA)

FIA_ATD.1	The Security Management server maintains a user database, containing accounts for administrators and authenticated users. Each account record contains the user's identity, supported authentication mechanisms, and for administrators: association with an administrator role, and a granular set of administrator authorizations (termed permissions). In order to substantiate the required roles, the evaluated configuration guidance provides instructions for the definition of two permissions profiles: an authorized administrator that may perform all management operations, and an authorized audit administrator that may only review audit trail and IDS System data. User certificates are stored in a separate ICA database on the Security Management server. Remote access VPN users may be associated in the user database with user groups, which can be used as a parameter in packet inspection rule base rules. User attributes for unauthenticated users are not maintained explicitly by the TOE. Note that the TSF does maintain topology definitions that are used to verify that the user's presumed identity match the logical interface and/or VPN domain from which the user binds to the TOE. Unauthenticated users' authorizations are considered to be those of a non-administrator, and group memberships bound implicitly in accordance with FIA_USB.1 /Admin.
FIA_UAU.1	FIA_UAU.1 describes all TOE interfaces that do not require prior user authentication. See discussion of supported authentication mechanisms below under FIA_UAU.5.
FIA_UAU.4	Administrators and VPN peers authenticate to the TOE using certificate-based authentication mechanisms, performed over the IKE and TLSv1.0 protocols, as described for FTP_TRP.1 and FTP_ITC.1. Both protocols prevent reuse of authentication data. 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. 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.
FIA_UAU.5	Administrators authenticate via the management GUI to the Security Management server installation. Prior to authentication, Security Management does not allow any interaction with the administrator. A SIC-based trusted path is established between the management GUI and the Security Management server. Administrator authentication is performed either via ICA-issued SIC certificates, or by configuring Security Management to forward the user's identity and password to an external authentication server, using RADIUS or SecurID protocols. The administrator's authentication mechanism is registered in the user database. OPSEC API clients always establish the SIC session using ICA certificates. Users sending or receiving information through the TOE can be authenticated by setting up a VPN rule that requires a remote access VPN tunnel to be used by the user for sending information through the TOE. The authentication mechanisms supported for remote access VPN

Component	Description of mechanism
	users are described above for FCS_CKM.2 /IKE. These include certificates, IKE pre-shared secrets, and 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 latter purpose. The TOE also supports an L2TP client-initiated exchange over an established IKE/IPsec trusted channel, in accordance with [RFC2661] and [RFC3193]. The IKE-authenticated identity is considered to be that of the Remote Access VPN client computer. The user identity transferred as part of the L2TP session establishment is authenticated via certificate-based authentication over the TLSv1.0 protocol (as described above for FCS_CKM.2 /TLS) in accordance with [RFC2716] (EAP-TLS), or with a user-entered password, transferred in accordance with [RFC1334] (PAP). In the latter case, the gateway sends the user's presumed identity and password to an authentication server in the IT environment in order to authenticate the user. TOE evaluated configuration guidance requires that only single-use password mechanisms be used. The external IT entities identified in this ST that must access the TOE are peer IPsec VPN gateways and hosts, NTP servers that are authorized to synchronize the TOE's time and date, and RADIUS[31] 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. NTP and RADIUS servers authenticate via single-use authenticators defined in the NTP and RADIUS protocols, respectively.
FIA_UID.2	The TOE relates to several types of users, as identified for FIA_USB.1 /Admin and FIA_USB.1 /IFF: administrators (corresponding to the security roles defined in FMT_SMR.1), unauthenticated users sending information through the TOE, authenticated remote access VPN users, and external IT entities. 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 IPsec 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.
FIA_USB.1 /IFF, FIA_USB.1 /Admin	Binding of user to subject occurs on a gateway when a packet is received for processing, and in Security Management for initiation of administration and OPSEC client sessions. The gateway implements user-subject binding by associating a VSID with each packet, and storing it in the connection table, together with other user relevant user identities: presumed

[31] Communication with SecurID authentication servers is constrained in the TOE evaluated configuration. A SecurID authentication server must be installed on a protected subnet. The TOE prevents any access to the authentication server by untrusted users. TOE components communicating with the authentication server must be either physically connected to the protected subnet, or use TOE VPN facilities to protect communications to the protected subnet. The TOE initiates all communications to the authentication server, for authenticating user single-use passwords. Therefore, the interface with the SecurID authentication server is considered to be a call-out from the TOE rather than an external user-visible interface, and is therefore exempt from the single-use authentication requirement for the external IT entity.

Component	Description of mechanism
	source address, and remote access VPN user identity (if available). For L2TP sessions, both user identity and client computer identity are bound to the subject and associated with auditable events. The Security Management maintains active administrator sessions, and associate user identity and authorizations for each session. User identity is also recorded in all relevant audit records.

7.1.5. Security Management (FMT)

FMT_MOF.1, FMT_MSA.1 /Attr, FMT_MSA.1 /MAC, FMT_MSA.1 /Rule, FMT_MSA.1 /VPN, FMT_MTD.1, FMT_SMF.1

As described in section 1.5.3.12, TOE security management is performed using management GUI applications that connect to the Security Management server installation. The authorized administrator role and authorized audit administrator role correspond to administrators using the SmartConsole GUI applications, with either full or restricted read-only log review privileges, respectively. The OPSEC client role corresponds to users connecting to the TOE using non-TOE applications that use the client APIs described in section 1.5.3.14.

As described for FTP_TRP.1 below, the TOE provides a trusted path for administration, based on the Secure Internal Communications (SIC) facility. The administrator must authenticate to Security Management using either certificate-based authentication or via a password that is authenticated with the support of an authentication server in the IT environment, using the RADIUS or SecurID protocols. SIC protects management communications from disclosure or modification. Thus only authenticated administrator roles may perform management operations.

Gateways also receive management commands from Security Management over authenticated, SIC-protected channels. Administrators do not connect to gateways for performing management operations.

Once the TOE is operational, there is no management role that requires access to any local or remote console interfaces that might otherwise have been used to bypass management interface protection mechanisms through direct access to operating system interfaces.

The management restrictions in the referenced SFRs are described in further detail in Table 7-3 below, derived from Table 6-3. For each management function in the table, the Management Functionality column describes the administrator interfaces and roles that may be used to invoke the function. Only the listed roles may do so.

Table 7-3- Management GUI Management Functions

Component	Management Function	Management Functionality
FMT_MOF.1	start-up and shutdown	Gateway start-up and shutdown are restricted to no administrator role in the TOE evaluated configuration because there is no administrator interface that allows the authorized administrator to perform these actions.
	enable, disable the operation of the TOE	
	create, delete, modify, and view default information flow security policy rules that permit or deny information flows	The authorized administrator can enable/disable the implied rules through the SmartDashboard Management GUI, as well as override them with alternative rules.
	create, delete, modify,	Administrator accounts and administrator SIC

Component	Description of mechanism		
		and view user attribute values defined in FIA_ATD.1	certificates are managed by the authorized administrator using SmartDashboard.
		enable and disable single-use authentication mechanisms in FIA_UAU.4 and FIA_UAU.5	SIC certificates for administrators are managed by the authorized administrator using SmartDashboard. Authentication of VPN peers is configured by the authorized administrator from SmartDashboard, including trusted CAs and certificate revocation distribution points, as well as IKE pre-shared secrets. SmartDashboard is also used for configuration of VPN community security attributes. Certificates used for NTP authenticators are set up during installation and generation of the TOE and cannot be modified by an 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 SmartDashboard Objects Database. An authorized administrator can configure RADIUS and SecurID server objects in the SmartDashboard Objects Database and require single-use password authentication for specific users or user groups.
		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.
		audit trail management	The SmartView Tracker management GUI allows the authorized administrator to perform log switches (changing the output log file), export log records out of the TOE for backup, and to purge the active log file. SmartView Tracker also provides audit trail review capabilities.
		archive, create, delete, and empty the audit trail	
		review the audit trail	SmartView Tracker allows the authorized administrator and authorized audit administrator roles to review audit trail data, including search and filter capabilities on displayed attributes. OPSEC clients access audit records via non-TOE applications using the LEA OPSEC API (see section 1.5.3.14). LEA is a well-defined API that

Component	Description of mechanism		
			provides log record information, including a data dictionary that assists the application in interpreting the information.
		backup of user attribute values, information flow security policy rules, and audit trail data, where the backup capability is supported by automated tools	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 management GUIs allow the authorized administrator to create backup copies of TSF data, user database, and information flow rules within the Security Management server, and to revert to a previous revision from these files. SmartView Tracker can be used to export audit trail data for backup purposes.
		recover to the state following the last backup	
		enable and disable remote administration from internal and external networks	Remote administration is enabled and disabled by setting up applicable Rule Base rules allowing control connections, using SmartDashboard.
		restrict addresses from which remote administration can be performed	Information security policy rules created by the authorized administrator in SmartDashboard restrict possible remote administration addresses.
		modify the behaviour of the functions of System data collection, analysis and reaction	SmartDashboard allows the authorized administrator to define information flow control rules and IDS/IPS behavior that control System data collection, analysis and reaction. The authorized administrator can also configure IPS Updates using the SmartDashboard management GUI.
		enabling SIC trust between Security Management and Security Gateway	Enabling SIC connectivity between Security Management and Security Gateway is performed during installation and generation of the gateway, in conjunction with corresponding definitions entered by the authorized administrator in the SmartDashboard management GUI.
	FMT_MSA.1 /Attr	delete attributes from a rule, modify attributes in a rule, add attributes to a rule	The authorized administrator creates and deletes information flow control rules and manages rule attributes using SmartDashboard, including firewall, NAT, IPS, and VPN functionality.

Component	Description of mechanism		
	FMT_MSA.1 /MAC	query, modify Virtual System interface and Customer associations	An authorized administrator manages Virtual Systems and interface allocations using the SmartDashboard management GUI. Default information flow security rules are specified as implied rules or as explicit low-priority catchall rules created by the administrator.
	FMT_MSA.1 /Rule	delete and create information flow rules described in FDP_IFF.1	
	FMT_MSA.1 /VPN	management of VPN rules	
	FMT_MSA.3	specification of default information flow security rules	
	FMT_MTD.1	query, modify, delete, and assign the user attributes defined in FIA_ATD.1.1	Administrator accounts and permissions profiles are managed by the authorized administrator using SmartDashboard.
		set the time and date used to form the timestamps in FPT_STM.1.1	Setting the time and date is restricted to no administrator role in the TOE evaluated configuration because there is no administrator interface that allows the authorized administrator to perform these actions.
		query IDS System and audit data	The SmartView Tracker management GUI allows the authorized administrator and authorized audit administrator to review audit log records. OPSEC clients access audit records and IDS System data via non-TOE applications using the LEA OPSEC API (see section 1.5.3.14). LEA is a well-defined API that provides log record information, including a data dictionary that assists the application in interpreting the information.
		add IDS System and audit data	OPSEC clients can use the ELA and AMON APIs for adding IDS System and audit data.
		query and modify all other TOE data (other than IDS System and audit data)	The Management GUIs are used by the authorized administrator for querying and modifying all other TOE data.
		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.

Component	Description of mechanism
	Gateway fail-safe behavior in the event of storage exhaustion is configured using SmartDashboard.
FMT_MSA.3	A set of restrictive 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 using information flow control rules); The evaluated configuration also includes a set of restrictive implied rules that allow authenticated management traffic between Gateways and Security Management hosts. Any other information flows are denied by default. The authorized administrator can override these default rules. An authorized administrator manages Virtual Systems and interface allocations using the SmartDashboard management GUI. Default values are restrictive in the sense that an interface is unavailable to all Virtual Systems until allocated to a virtual entity by an authorized System administrator.
FMT_SMR.1	The definition of the authorized management roles in the context of this ST is given in section 1.5.3.12. OPSEC client APIs are identified in section 1.5.3.14.

7.1.6. Protection of the TSF (FPT)

FPT_FLS.1	During initial start-up of a Gateway, the TOE verifies the integrity of stored executable code and security policy. The boot sequence is aborted if a failure is identified. The gateway starts processing information flow requests only after security policy enforcement is up and running. During normal operation, a watchdog kernel thread tests for the normal operation of critical hardware (e.g. NICs), system processes, the integrity of security policy information, and for connectivity between cluster members, as described below for FPT_TST.1. A non-recoverable failure will cause the gateway to transition to an error state, and to stop processing information flow requests until the failure is remediated. When this occurs, the TOE transitions standby virtual entities defined on other cluster members to the active state, as described below for FRU_FLT.2. TOE information flow control is fail-safe in the sense that it is default-deny, i.e. an information flow will be denied unless the gateway matches it against rule and state information that allows it.
FPT_ITT.1	All TOE internal management communications between the separate parts of the TOE[32] are protected from disclosure and modification by the Secure Internal Communications (SIC) security function. SIC protects all communications between management GUIs and Security Management, communications between multiple Security Management server hosts, and communications between Security Management server hosts and managed gateways. SIC is based on the TLSv1.0 protocol, using Triple DES encryption and RSA digital signatures

[32] As discussed below in sections 7.2.2 and 7.2.3, clustering synchronization traffic between cluster members is not cryptographically-protected over SIC. TOE guidance instructs that cluster members should be co-located, and they are therefore not considered 'separate' parts of the TOE.

Component	Description of mechanism
	for authentication (see above for FCS_CKM.2 /TLS). As described in section 1.5.3.13, SIC entities authenticate using ICA-issued certificates.
FPT_STM.1	The timestamps used for stamping audit records are provided by the underlying operating system that is part of the TOE on both Check Point Security Gateway Appliances and Check Point Security Management hosts. The operating system uses a hardware clock to maintain reliable time even after periods of time when the appliance or server is powered down. 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 configured Security Management 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. The TOE supports time synchronization by including an NTP polling agent that can be configured to interact with an authorized external time synchronization server, authenticated using certificate-based single-use autokey authenticators as defined in the NTPv4 protocol. There is no administrator interface for modifying the clock once the TOE is operational.
FPT_TDC.1	[802.1q] VLAN ID tags are mapped to TOE logical interfaces in accordance with the rules described in FDP_ITC.2. The TOE uses VLAN ID tags to map the packet to a defined logical interface.
FPT_TRC.1	Security policy information is replicated between all Security Management server hosts, whenever a new policy is saved and/or on a predefined schedule. Security Management server databases can be replicated from an active server to zero or more standby servers. All management operations such as editing and installing the Security Policy and modifying users and objects, are performed against the active Security Management server. If the active serveris unavailable, one of the standby servers should be made active. This transition from standby to active is initiated manually by the authorized administrator. Log records are not replicated between Security Management servers. In order to allow log review on both active and standby severs, Gateways can be configured to forward log records to multiple servers. The administrator installs the security policy on the cluster rather than separately on individual cluster members. The policy is automatically installed on all cluster members. When a failed cluster member recovers, it will first try to take a policy from one of the other cluster members. The assumption is that the other cluster members have a more up to date policy. If this does not succeed, it compares its own local policy to the policy on the Security Management server. If the policy on the server is more up to date than the one on the cluster member, the policy on the server will be retrieved. If the cluster member does not have a local policy, it retrieves one from the server. This ensures that all cluster members use the same policy at any given moment. If configured for state synchronization, cluster members synchronize state tables over dedicated synchronization networks, as described in section 1.5.1.6. State synchronization allows sub-second failover to a standby cluster member in high availability configurations, by ensuring that the standby member maintains a copy of the active state tables including all active connections. State synchronization also supports load balancing configurations, where an incoming packet can be processed by any cluster member. In order to prevent race conditions such as a TCP SYN+ACK response being processed by another cluster member before the original SYN packet state update arrives from the member that processed it, the TOE implements a hold and flush paradigm, i.e. in the preceding example, the SYN packet is put on hold and not released to flow

Component	Description of mechanism
	to its intended target, before all cluster members acknowledge the state update. When a cluster member recovers from a failure or starts up initially, it performs a Full Synchronization over a SIC-protected TCP session from another active cluster member. It enters an active state and starts processing information flow requests only after state synchronization has completed successfully. Cluster members in active or standby states exchange state updates over the dedicated synchronization networks, using a reliable UDP-based Check Point proprietary Cluster Control Protocol (CCP).
FPT_TST.1	During initial start-up of a Security Gateway, the TOE verifies the integrity of stored executable code, by computing an error detection code as a function of all executable files on the gateway, and comparing it to a stored value. Policy files are verified when they are received from the Security Management server against a SHA-1 hash included in the policy file. The integrity of the policy file is also verified during gateway startup. If an integrity error is detected, the gateway will not initiate information flow control processing. During initial gateway startup and periodically during normal operation, a watchdog kernel thread monitors the existence of critical processes. A cluster member is considered to have failed when any of the monitored entities reports an error or fails to report its status. By default, monitored entities include: cluster interfaces on cluster members, full synchronization status, the security policy load status, and the existence of critical gateway daemons. Additional monitored entities may be registered during gateway initialization. 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. Administrators can determine that managed appliances are in operational status via the SmartView Monitor Management GUI.
7.1.7. Fault tolerance (FRU)	
FRU_FLT.2	As described above for FPT_TST.1, gateways peform self-tests for verifying the the normal operation of critical hardware and software entities. A non-recoverable failure will cause the gateway to transition to an error state, and to stop processing information flow requests. When this occurs, the TOE transitions standby virtual entities defined on other cluster members to the active state, as described in section 1.5.3.15. The cluster redirects subsequent packets to the newly active virtual entities. This ensures that all TOE capabilities are retained. Multiple Security Management servers synchronize security policy and user databases using Management High Availability functionality, so that if the active server fails, an authorized administrator can manually transition a standby server to the active mode. As described above for FAU_GEN.1, in a management high-availability configuration the gateway can forward its log records to both active and standby Security Management servers to ensure that log data is accessible on both active and standby Security Management servers.
7.1.8. Trusted path/channels (FTP)	
FTP_ITC.1	As described above for FCS_CKM.2 /IKE, the TOE's IKE/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. As described above for FCS_CKM.2 /TLS, the TOE's 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. Only the remote access VPN

Component	Description of mechanism
	client can initiate the TLS session with the TOE
FTP_TRP.1	Administration of the TOE is performed over SIC channels between the management GUI and the Security Management server, providing assured identification of the two end points and protection of the communicated data from modification or disclosure.

7.1.9. Intrusion Detection (IDS)

IDS_ANL(EXP).1	As described in section 1.5.3.8, network traffic that has been allowed by the firewall and VPN security policies is compared against signature events encoded as regular expressions and INSPECT language code. INSPECT is an object-oriented, high-level script language that specifies packet handling by classifying packet content and state. INSPECT scripts are compiled by a Security Management Server into low-level inspection code that is executed on Security Gateways using a kernel-level stack-based virtual machine. An INSPECT script applies a conditioned sequence of pattern matching operations on packets flowing through the gateway. An INSPECT operator can be used to enforce an information flow control decision (i.e. permit or deny the information flow), generate log records, and can read and modify state information encoded in transient registers and in persistent state tables. 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 SFRs. Compound Signature Identification supports matching of sequences of events. Encoded signature events can be set to log the detected potential violation. Check Point Security Gateway Appliances record within each analytical result (manifested as a match against an IPS protection) 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_RCT(EXP).1	When an intrusion is detected, i.e. when incoming traffic matches an IPS protection, the authorized administrator configures the gateway to log the event and/or drop the suspected traffic. Auditable events are configured by the authorized administrator to generate alerts when an intrusion is detected. 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.
IDS_RDR(EXP).1	IDS System data is collected as event log records, and consolidated with the TOE's audit trail in the Security Management server log database. Administrators review the logs in human readable form using SmartView Tracker. Only authenticated administrators and OPSEC clients are allowed access to the Security Management server installation in order to review audit logs.
IDS_SDC(EXP).1	IDS System data is collected as event log records, and consolidated with the TOE's audit trail in the Security Management server log database. The Gateway collects the following information from network traffic flowing through the TOE: service requests (access to network services), network traffic, and detected known vulnerabilities (matched IPS protections). 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),

Component	Description of mechanism
	and in addition: protocol, service, and destination address. For detected known vulnerabilities, the identification of the known vulnerability is the name of the rule matched by the traffic.
IDS_STG(EXP).1, IDS_STG(EXP).2	IDS System data is collected as event log records, and consolidated with the TOE's audit trail in the Security Management server log database. The fulfillment of the IDS_STG(EXP).1 and IDS_STG(EXP).2 requirements therefore corresponds to the description given above for FAU_STG.2 and FAU_STG.4. Audit records are protected from unauthorized deletion and unauthorized modifications. The TSF ensures that all stored audit records are maintained in case of audit storage exhaustion, failure and/or attack, and that only a limited number of records that have not yet been stored might be lost in case of failure or attack. Gateways are configured to stop mediating network traffic when storage space is exhausted. 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.

7.2. Protection against Interference and Logical Tampering

7.2.1. 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 Security Gateway Appliances gateway, that prevents any external access to these components.

7.2.2. Protection of Clustering Synchronization Information

Synchronization information exchanged between cluster members is protected by the use of dedicated synchronization interfaces. TOE guidance provides instructions for the secure installation of the cluster. As cryptographic mechanisms are not used for protecting cluster synchronization traffic, cluster members should be co-located.

The TOE handles cluster synchronization protocol traffic received on non-synchronization interfaces in accordance with information flow control policy, and does not regard it as cluster synchronization information.

7.2.3. Trusted Path and Trusted Channels

All internal TOE communications (except for clustering synchronization information – see section 7.2.2) are protected by the Secure Internal Communications (SIC) facility, preventing unauthorized users from tampering with the communications between distributed TOE components.

7.2.4. Self Testing

When the Check Point Security Gateway Appliances gateway is started, it 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 by the Security Gateway when they are received from the Security Management server. Software integrity is verified during startup. Administrators can determine that managed appliances are in operational status via the SmartView Monitor management GUI.

7.3. Protection against Bypass

7.3.1. Virtual Defragmentation

When IPv4 packets that are fragmented are received by the Check Point Security Gateway Appliances gateway, they are first reassembled before being inspected. Only well-formed packets are passed on to packet inspection and IPS analysis.

7.3.2. Residual Information Protection

All buffers containing packet information and cryptographic keying material are cleared before being allocated, thus preventing residual information leakage.

7.3.3. Boot Security

During the Check Point Security Gateway Appliances gateway 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.

7.3.4. Reference Mediation

All network traffic arriving or departing at a TOE network interface is mediated by the TSF once the Check Point Security Gateway Appliances gateway is in an operational state.

All management interfaces use a common authentication, authorization, and auditing mechanism, preventing administrators from attempting to exceed their authorizations by bypassing security controls.

TOE evaluated configuration guidance requires that administrators should not be given access to TOE operating system interfaces once the TOE is operational, thereby preventing the threat of bypass of the TSF via these interfaces.

8. Supplemental Information

8.1. References

The following external documents are referenced in this Security Target.

Identifier	Document
[802.1Q]	IEEE Standard for Local and metropolitan area networks – Virtual Bridged Local Area Networks, IEEE Std 802.1Q-2005, 19 May 2006.
[APP-PP]	U.S. Government Protection Profile for Application-level Firewall In Basic Robustness Environments, Version 1.1, July 25, 2007
[CAPP]	Controlled Access Protection Profile, Version 1.d, October 8, 1999
[CC]	Common Criteria for Information Technology Security Evaluation Parts 1-3, Version 3.1, Revision 3, September 2009, CCMB-2009-07-001, 002 and 003
[CEM]	Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, Version 3.1 Revision 3, September 2009, CCMB-2009-07-004
[ConfigMode]	INTERNET DRAFT draft-dukes-ike-mode-cfg-02.txt – The ISAKMP Configuration Method, September 2001
[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
[FIPS186-2]	NIST FIPS 186-2 with Change Notice 1, Digital Signature Standard, October 5, 2001
[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
[HybridMode]	INTERNET DRAFT draft-ietf-ipsec-isakmp-hybrid-auth-05.txt – A Hybrid Authentication Mode for IKE, August 2000
[I-0356]	NIAP Interpretation I-0356: FDP_RIP Annex: Reuse Of Subject Data Notes
[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-0421]	NIAP Interpretation I-0421: Application Notes in Protection Profiles Are Informative Only
[I-0422]	NIAP Interpretation I-0422: Clarification of "Audit Records"

[I-0427] NIAP Interpretation I-0427: Identification of Standards

[IDSSPP] U.S. Government Protection Profile Intrusion Detection System System for Basic Robustness Environmemts, Version 1.7, July 25, 2007

[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-0036] NIAP Precedent Decision PD-0036: Distinction between Internal and External Networks in a Firewall PP

[PD-0055] NIAP Precedent Decision PD-0055: Effect of Addition of Environmental Assumptions on PP Compliance

[PD-0067] NIAP Precedent Decision PD-0067: For the Controlled Access Protection Profile (CAPP), must all events be pre-selectable? Post-selectable?

[PD-0071] NIAP Precedent Decision PD-0071: Identification of Operations on Security Functional Requirements

[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

[PD-0131] NIAP Precedent Decision PD-0131: Create Object Audit Event and CAPP Compliance

[PD-0136] NIAP Precedent Decision PD-0136: Using CCv2.x PPs with CCv3.1 STs: Handling of FPT_SEP and FPT_RVM

[PD-0139] NIAP Precedent Decision PD-0139: CC V3 Conformance Type for Existing CC V2 PPs

[PD-0151] NIAP Precedent Decision PD-0151: Acceptable Demonstrable Assurance for the IDS System PP v1.7 (BR)

[PPFWTFMR] U.S. Government Traffic-Filter Firewall Protection Profile for Medium Robustness Environments, Version 1.1, July 25, 2007

[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

[RFC1334] RFC 1334 - PPP Authentication Protocols, October 1992

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

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

[RFC1994] RFC 1994 - PPP Challenge Handshake Authentication Protocol (CHAP), August 1996

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

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

[RFC2284] RFC 2284 - PPP Extensible Authentication Protocol (EAP), March 1998

[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

[RFC2631] RFC 2631 – Diffie-Hellman Key Agreement Method

[RFC2661] RFC 2661 – Layer Two Tunneling Protocol "L2TP", August 1999

[RFC2716] RFC 2716 - PPP EAP TLS Authentication Protocol, October 1999

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

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

[RFC3193] RFC 3193 – Security L2TP using IPsec, November 2001

[RFC3526] RFC 3526 – More Modular Exponential (MODP) Diffie-Hellman groups for Internet Key Exchange (IKE)

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

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

[RFC4330] RFC 4330 – Simple Network Time Protocol (SNTP) Version 4 for IPv4, IPv6 and OSI, January 2006

[RFC4346] RFC 4346 – The Transport Layer Security (TLS) Protocol Version 1.1, April 2006

[RFC4753] RFC 4753 – ECP Groups for IKE and IKEv2, January 2007

[RFC4868] RFC 4868 – Using HMAC-SHA-256, HMAC-SHA-384, and HMAC-SHA-512 with IPsec, May 2007

[RFC5114] RFC 5114 – Additional Diffie-Hellman Groups for Use with IETF Standards, January 2008

[RFC5246] RFC 5246 – The Transport Layer Security (TLS) Protocol Version 1.2, August 2008

[RFC5996] RFC 5996 – Internet Key Exchange Protocol Version 2 (IKEv2), September 2010

[RI#137] Final Interpretation for RI # 137 – Rules governing binding should be

specifiable, CCIMB, January 30, 2004

[SP800-38A] NIST Special Publication 800-38A, Recommendation for Block Cipher Modes of Operation – Methods and Techniques, December 2001

[SP800-38D] NIST Special Publication 800-38D, Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC, November 2007

[SP800-67] NIST Special Publication 800-67, Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher, May 19, 2008

[SP800-90] NIST Special Publication 800-90, Recommendation for Random Number Generation Using Deterministic Random Bit Generators (Revised), March 2007

[TFF-PP] U.S. Government Protection Profile for Traffic Filter Firewall In Basic Robustness Environments, Version 1.1, July 25, 2007

8.2. 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.

8.2.1. 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”.
- Protected assets are denoted by the prefix “D.”, e.g. “D.PACKET”.
- Subjects are denoted by the prefix “S.”, e.g. “S.VS”.
- Users are denoted by the prefix “U.”, e.g. “U.ADMIN”.

8.2.2. 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, 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.

8.2.2.1. 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 slash and an iteration name, e.g. “/DAC”. These follow the short family name and allow components to be used more than once with varying operations.

8.2.2.2. 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.

8.2.2.3. 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.

8.2.2.4. 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.

8.2.3. Other Notations

8.2.3.1. 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 5. 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.

8.2.3.2. 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.

8.2.3.3. Footnotes

Footnotes[33] are used to provide further clarification for a statement, without breaking the flow of the text.

8.2.3.4. 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 4.2.

[33] This is an example of a footnote.

8.2.4. Highlighting Conventions

The conventions for SFRs described above in sections 8.2.2 and 8.2.3 are expressed in chapter 6 by using combinations of bolded, italicized, and underlined text as specified in Table 8-1 below.

Assignments, selections, and refinements that were already performed in the claimed PPs 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 more than one PP, these conventions are applied in relation to only one PP, with the following precedence (except where otherwise noted): [IDSSPP], [TFF-PP], [APP-PP]. The operations performed on the requirement component in relation to the other PP(s) are not identified using a highlighting convention, to avoid confusion. Note that all operations performed in relation to each of the PPs are identified in Table 6-1.

Table 8-1- SFR Highlighting Conventions

Convention	Purpose	Operation
Boldface	Boldface text denotes completed component assignments. Example: *6.2.2.5 Cryptographic operation (FCS_COP.1 /ESP)* FCS_COP.1.1 The TSF shall perform **encryption and decryption of IPsec 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: *6.2.6.1. Basic internal TSF data transfer protection (FPT_ITT.1)* FPT_ITT.1.1 The TSF shall protect TSF data from <u>disclosure</u> and <u>modification</u> when it is transmitted between separate parts of the TOE.	(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: *6.2.5.5. 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: *6.2.3.3. Subset information flow control (FDP_IFC.1 /TFF)* FDP_IFC.1.1 The TSF shall enforce the TRAFFIC FILTER SFP on: *6.2.3.4. Subset information flow control (FDP_IFC.1 /VPN)* FDP_IFC.1.1 TSF shall enforce the VPN SFP on:	Iteration 1 (FDP_IFC.1) Iteration 2 (FDP_IFC.1)
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

8.3. Terminology

The Common Criteria defines many terms that are used in the specification of Security Targets (STs). 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 Security Gateway Appliances product.

8.3.1. 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[34] and the disclosure and modification of data.[35]

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

Administrator An entity that has complete trust with respect to all policies implemented by the TSF.

Assurance Grounds for confidence that a TOE meets the SFRs.

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 the claimed identity of a user.

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

Authorised user An authenticated user who may, in accordance with the TSP, perform an operation.

[34] Hardware and software.

[35] Stored or communicated.

Availability Timely[36], reliable access to IT resources.

ClusterXL Check Point proprietary clustering technology that synchronizes state tables and distributes packet processing across cluster members, supporting high availability failover and load balancing configurations.

Compromise Violation of a security policy.

Confidentiality A security policy pertaining to disclosure of data.

CoreXL Check Point proprietary acceleration technology that distributes security processing across multiple processing cores.

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 entity any entity (human or IT) outside the TOE that interacts (or may interact) with the TOE.

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.

[36] According to a defined metric.

- The name used to refer to a specific instance of the object must exist in a context that potentially allows subjects with 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 A passive entity in the TOE, that contains or receives information and upon which subjects perform operations.

Operation A specific type of action performed by a subject on an object.

Operational Environment

The environment in which the TOE is operated. 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.

Organizational Security Policy

A set of security rules, procedures, or guidelines imposed (or presumed to be imposed) now and/or in the future by an actual or hypothetical organization in the operational environment.

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 attribute A property of subjects, users (including external IT products), objects, information, sessions and/or resources that is used in defining the SFRs and whose values are used in enforcing the SFRs.

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 Security Management server

IPS 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 A Virtual Private Network implementation based on the IKE/IPsec protocols.implementation based on the TLS protocol.

Subject An active entity in the TOE that performs operations on objects.

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.

TOE Security Functionality

A set consisting of all hardware, software, and firmware of the TOE that must be relied upon for the correct enforcement of the SFRs.

Trusted Channel A means by which a TSF and a remote trusted IT product can communicate with necessary confidence.

Trusted Path A means by which a user and a TSF can communicate with necessary confidence.

User Any entity (human user or external IT entity) outside the TOE that interacts with the TOE.

Virtual Private Network A framework for establishing cryptographically protected secure channels between network entities that protect information from disclosure and modification while in transit over the network.

VPN domain The set of addresses defined to be ‘internal’ in a Security Gateway’s topology.

Vulnerability A weakness in the TOE that can be used to violate the SFRs in some environment.

8.3.2. 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
MIB	Management Information Base
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

Abbreviation	Description
SSL	Secure Sockets Layer
ST	Security Target
TCP	Transmission Control Protocol
TLS	Transport Layer Security
TOE	Target of Evaluation
TSF	TOE Security Functionality
TSS	TOE Summary Specification
UDP	User Datagram Protocol
VLAN	Virtual LAN
VM	Virtual Machine
VPN	Virtual Private Network
VRF	Virtual Route Forwarding
VS	Virtual System
VSID	Virtual System Identity

Appendix A - TOE Hardware Platforms

A.1. Supported Open Server Hardware for Check Point Gaia

The following commodity hardware platforms are included in the evaluated configuration for Security Gateway and Security Management software, running the Gaia R77 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**:
  - AMD Opteron® or Intel XEON® processor configurations
  - Other processors that are code-compatible with the listed configurations[37]
- Intel Pentium IV or 2 GHz or higher code-compatible equivalent processor configurations
- **Memory**: a minimum of 500 MB (1 GB for Security Management servers)
- **Mass Storage**: a minimum of 10 GB
- **Network controllers**: the following adapter families are included:

Chipset	Driver	Included Adapters
Intel® 825xx	e100	Any adapter from the Intel® Pro/100 family
	e1000, e1000e, igb, ixgbe	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, tg3	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, sky2	Any adapter based on a Marvell Yukon 88E80xx Gigabit Ethernet controller

[37] Check Point FIPS 140-2 testing was performed on specific processor configurations listed in the non-proprietary FIPS 140-2 Security Policy documentation. 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**:

Vendor	Model
Check Point	IAS Server L2, L6, L8, M2, M6, M8, D1, D2, D6, D8, R1, R2, R6, R8, U1
Dell	PowerEdge 620, 720
Fujitsu	Primergy RX100 S6, S7
	Primergy RX200 S6, S7
	Primergy RX300 S6, S7
HP	ProLiant DL120 G7
	ProLiant DL320e G8
	ProLiant DL360 G7
	ProLiant DL380 G7
	ProLiant DL360p G8
	ProLiant DL380p G8
IBM	System X x3550 M3, M4
	System X x3650 M3, M4

A.2. Supported Check Point Security Gateway Appliances

The following Check Point security appliance models are included in the evaluated configuration for the Security Gateway software. Each appliance model is identified using a Check Point security appliance family name (Power-1, UTM-1, or Check Point Appliance) and model number (e.g. 507*).

Note: The '*' in the model number stands for the number of software blades normally licensed for the given appliance, e.g. the 'Power-1 5075' model would correspond to an appliance from the Check Point Power-1 security appliance family model 507*, with up to five (5) licensed software blades. The models identified using the '**' convention use a zero-justified numbering system for the licensed software blades, e.g. the 'Check Point 21412 Appliance' would support up to 12 software blade licenses, whereas the 'Check Point 21407' Appliance' would be the same hardware model supporting up to 7 blades.

- Power-1 507*
- Power-1 907*
- Power-1 1106*, 1107*, 1108*
- UTM-1 27*, 57*
- UTM-1 107*, 207*, 307*
- Check Point 22** Appliances

- Check Point 42**, 44**, 46**, 48** Appliances
- Check Point 122**, 124**, 126**, 135** Appliances
- Check Point 214**, 216**, 217** Appliances
- VSX-1 3070 Appliances
- VSX-1 9070 Appliances
- VSX-1 9090 Appliances
- VSX-1 11000 series Appliances
- VSX-1 11200 series (VSLS) Appliances
- Check Point 12200 VSX Appliances
- Check Point 12400 VSX Appliances
- Check Point 12600 VSX Appliances
- Check Point 21400 VSX Appliances

These appliances run Check Point Security Gateway Appliances, on an appliance-specific build of the Gaia R77 operating system.

A.3. Supported Check Point IP Appliances

The following IP Appliance[38] models are included in the evaluated configuration for the security policy enforcement software (gateways), running the Gaia R77 operating system:

- IP295
- IP395
- IP565
- IP695
- IP1285
- IP2455

A.4. Supported Check Point Security Management Appliances

The following Check Point security appliance models are included in the evaluated configuration for the Security Management software, running the Gaia R77 operating system:

- Smart-1 5
- Smart-1 25

[38] The IP152, IP295, IP395, IP565, IP695, IP1285, and IP2455 appliances are Check Point re-branded instances of the previously Nokia-branded IP150, IP290, IP390, IP560, IP690, IP1280, and IP2450, respectively.

- Smart-1 50
- Smart-1 150