totalsecurity™

Check Point SOFTWARE TECHNOLOGIES LTD.

Check Point VSX

Security Target

Version 1.1

May 20, 2012

Prepared for:

Check Point SOFTWARE TECHNOLOGIES LTD.

5 Ha'Solelim St.

Tel Aviv, Israel 67897

Prepared by:

Metatron Security Services

Metatron Security Services Ltd.

66 Yosef St.,

Modiin, Israel 71724

All marks, trademarks, and logos mentioned in this material are the property of their respective owners.

©2012 Check Point Software Technologies Ltd. All Rights Reserved.

Classification: [Unrestricted]—For everyone

Document Version Control Log

Version	Date	Author	Description
0.1	June 11, 2009	Nir Naaman	Initial CCv3.1 version.
0.7	October 15, 2009	Nir Naaman	Post-iVOR validator-requested updates.
0.95	November 9, 2011	Nir Naaman	Updated TOE software version to VSX R67.10.20 in combination with Provider-1 R71 with R7x hotfix. Added supported VSX appliances.
1.0	February 15, 2012	Nir Naaman	Updated list of supported Open Servers. Referenced updated evaluated configuration guidance.
1.1	May 20, 2012	Nir Naaman	Referenced final evaluated configuration guidance.

©2012 Check Point Software Technologies Ltd. All Rights Reserved.

Classification: [Unrestricted]—For everyone

Table of Contents

©2012 Check Point Software Technologies Ltd. All Rights Reserved.
Classification: [Unrestricted]—For everyone

©2012 Check Point Software Technologies Ltd. All Rights Reserved.

Classification: [Unrestricted]—For everyone

©2012 Check Point Software Technologies Ltd. All Rights Reserved.

Classification: [Unrestricted]—For everyone

List of Tables

©2012 Check Point Software Technologies Ltd. All Rights Reserved.

Classification: [Unrestricted]—For everyone

List of Figures

©2012 Check Point Software Technologies Ltd. All Rights Reserved.
Classification: [Unrestricted]—For everyone

©2012 Check Point Software Technologies Ltd. All Rights Reserved.

Classification: [Unrestricted]—For everyone

1. ST Introduction

1.1. ST Reference

Title:	Check Point VSX Security Target
ST Version:	1.1
ST Date:	May 20, 2012
Author:	Nir Naaman
CC Version:	Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 3, July 2009
Assurance Level:	EAL 4, augmented with ALC_FLR.3 (systematic flaw remediation).
Keywords:	traffic filter, firewall, VPN, IPSec, SSL VPN, IDS/IPS, intrusion detection, virtualization, security management

1.2. TOE Reference

TOE Software Identification: Check Point VSX R67.10.20[1] in combination with Check Point Provider-1 R71 with R7x hotfix

TOE software also includes SmartConsole management GUI products that are installed on a standard PC (outside the TOE) running a Microsoft Windows operating system. The evaluated version for SmartConsole is: R71 with R7x hotfix.

TOE Hardware Identification:

The TOE consists of Check Point VSX software on an appliance platform running the Check Point SecurePlatform VSX operating system. The TOE includes the following classes of appliances:

- Open Server hardware platforms (listed in section A.1).
- Check Point VSX-1 security appliances (listed in section A.2).

Check Point Provider-1 software is always installed on a separate platform selected from the list given in section A.3, running the Check Point SecurePlatform operating system. The platform selected for this purpose is considered part of the TOE, but is not used in the identification of the TOE.

TOE Support Program Identification: Enterprise Software Subscription[2]

[1] The TOE software identification is a combination of the product name (Check Point VSX) and the product version (R67.10.20), which identifies the product's major version and a Hot Fix Accumulator (HFA) number. This combination uniquely identifies a software build for each of the supported appliance classes. Throughout this document, the product is referred to as Check Point VSX or VSX for short, omitting the version and HFA number.

[2] Enterprise Software Subscription (included in all Check Point Enterprise Support Programs) is required for receiving software upgrades, as part of Check Point's flaw remediation procedures.

©2012 Check Point Software Technologies Ltd. All Rights Reserved.

Classification: [Unrestricted]—For everyone

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.

©2012 Check Point Software Technologies Ltd. All Rights Reserved.

Classification: [Unrestricted]—For everyone

1.4. TOE Overview

1.4.1. Usage and Major Security Features of the TOE

Check Point VSX is a virtualization environment for the implementation of network traffic information flow controls, providing controlled connectivity between two or more network environments.

Clusters of one or more Check Point VSX gateways are typically connected to a large number of physical and/or virtual (VLAN) network interfaces located in the enterprise or service provider's network core. The gateways mediate information flows between clients and servers located on these attached networks, providing security functionality that includes traffic filtering, intrusion detection and prevention (IDS/IPS), IKE/IPSec and SSL virtual private networking (VPN), and network address translation (NAT).

Information flow control functionality is implemented by one or more *Virtual Systems*, each logically equivalent[3] to a Check Point Security Gateway appliance, Check Point's flagship perimeter security product. Each Virtual System is associated with two or more logical interfaces. Check Point VSX maintains 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. Information flows between Virtual Systems are allowed or denied by an authorized administrator using a Mandatory access control policy.

A Check Point Provider-1 installation consists of one or more Multi-Domain Server hosts that maintain multiple independent *Customer* management domains for managing disparate sets of Virtual Systems. Administrators connect to the Multi-Domain Server using the management GUIs, and are restricted to accessing only Customer domains for which they have been explicitly authorized.

Check Point VSX cluster members synchronize state tables, ensuring fault-tolerance with sub-second failover to a standby Virtual System.

Check Point VSX meets and exceeds the security requirements of two U.S. Government protection profiles, for 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 EAL 4 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.

[3] Some Check Point Security Gateway functionality is not available in the Check Point VSX product. For example, Security Servers (application-level proxies) are not supported. Such functionality is not claimed in this ST. Refer to the product release notes for a complete list of unsupported Security Gateway features.

©2012 Check Point Software Technologies Ltd. All Rights Reserved.

Classification: [Unrestricted]—For everyone

1.4.2. TOE Type

Check Point VSX is a virtualization environment for the implementation of network traffic information flow controls, providing controlled connectivity between two or more network environments. Users bind to a Virtual System by sending IP packets (datagrams) flowing between controlled networks so that they pass through the TOE. This allows TOE Virtual Systems to inspect, allow or deny and optionally modify these information flows, by running information flow control programs coded in Check Point's patented INSPECT language.

As such, the TOE type may best be characterized as that of an operating system. An operating system manages pools of physical resources (i.e. CPU, disk, network interfaces), abstracting them into logical objects. Subjects (Virtual Systems, Customers) are given controlled access to these objects. The operating system also provides controlled information flow services between subjects, using shared objects (virtual and physical network interfaces).

The TOE type also corresponds to the types of information flow controls provided by the TOE: firewall, NAT, VPN, and IPS.

The TOE 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. Excluded product types are extended configurations of the Check Point VSX product that are outside the TOE evaluated configuration. Column 3 of Table 1-1 specifies Check Point add-on products, licenses or configurations that provide the additional functionality.

Table 1-1 – Check Point VSX Product Types

Product Type	Scope	Dependencies
Operating System	☑	
Firewall / NAT gateway	☑	
IPSec VPN gateway	☑	
Remote access / SSL[4] VPN gateway	☑	
IDS/IPS appliance	☑	
Enterprise Security Management	✘	OSE, Eventia add-ons
Cooperative enforcement (NAC)	✘	Policy Server, Integrity Server add-ons
Certificate management (PKI)	✘	External access to Internal CA is blocked in evaluated configuration

Key: ☑ Claimed security functionality ✘ Excluded from TOE

[4] 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.

©2012 Check Point Software Technologies Ltd. All Rights Reserved.

Classification: [Unrestricted]—For everyone

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

1.4.3.1. Overview

The TOE includes management GUI applications: Provider-1 Multi-Domain GUI (MDG) and SmartConsole. SmartConsole is an integrated set of management GUI applications, including SmartDashboard, SmartView Tracker, and SmartView Monitor.

The management GUI applications are installed on standard PC administrator workstations running Microsoft Windows (workstation hardware and Windows operating system are not part of the TOE), and are used as the management interface for the TOE.

1.4.3.2. Software Required in the IT Environment

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

- Windows XP Home & Professional (SP3)
- Windows Vista (Ultimate, Enterprise, Business, Home Premium, or Home Basic) (SP1)
- Windows Server 2003 (Standard, Enterprise, or Datacenter Edition) (SP1-2)
- Windows Server 2008

1.4.3.3. Hardware Required in the IT Environment

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

©2012 Check Point Software Technologies Ltd. All Rights Reserved.

Classification: [Unrestricted]—For everyone

1.5. TOE Description

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

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

- Claimed security functionality that is evaluated in the context of this ST;
- Other functionality that is in the TOE but is not evaluated in the context of this ST except for the determination that it cannot compromise any claimed security functionality;
- Excluded functionality that is not available in the TOE's evaluated configuration[5].

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.
- **Example Deployment Strategies** – describes different configurations of the TOE that may be used by Check Point customers, demonstrating applications of the TOE's logical security features.

[5] 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.

©2012 Check Point Software Technologies Ltd. All Rights Reserved.

Classification: [Unrestricted]—For everyone

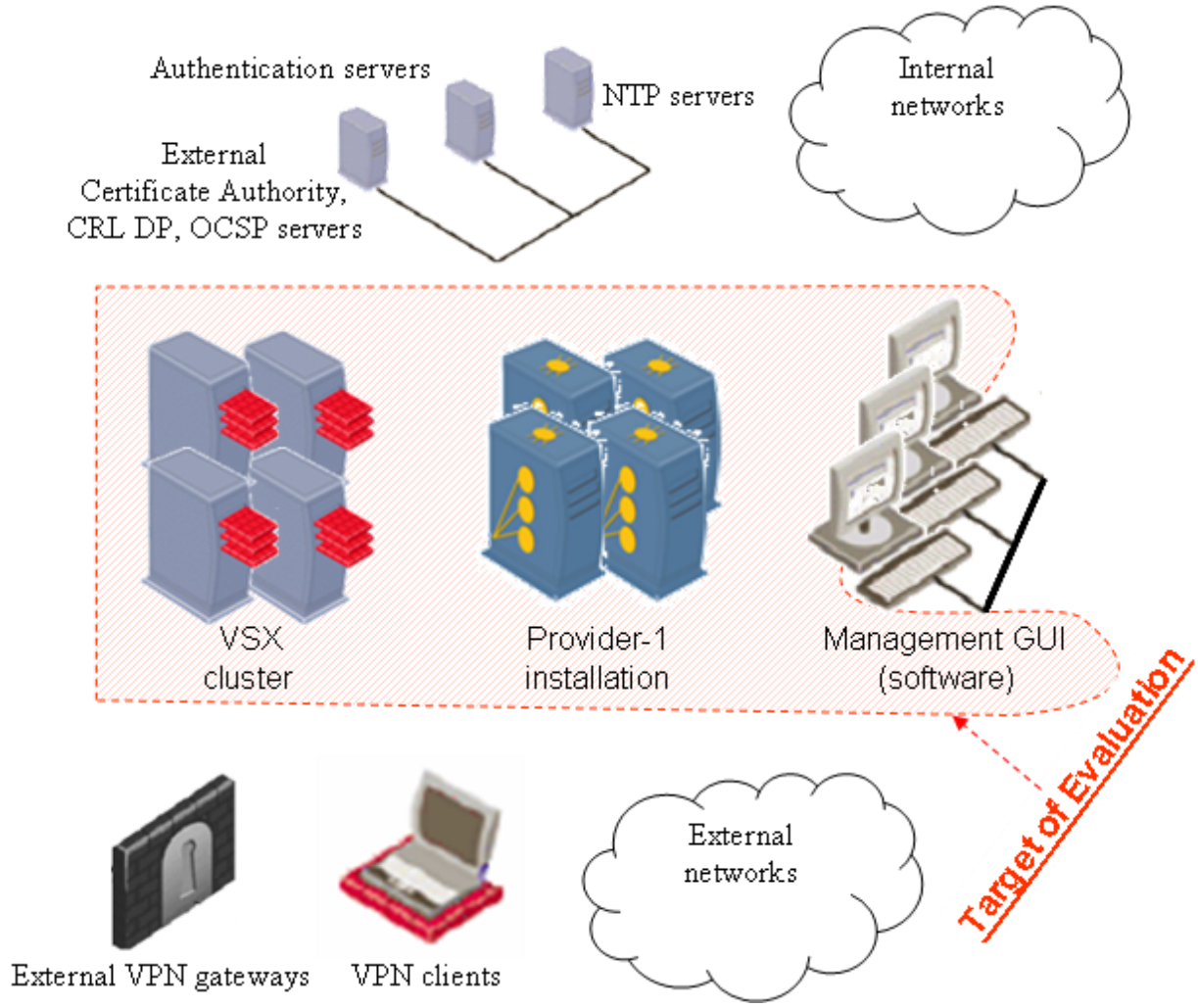
1.5.1. Physical Scope of the TOE

1.5.1.1. Definition

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

- Check Point VSX software, OS, and Hardware platform(s) on which the software is installed; and
- Check Point Provider-1 (Management) server software, OS and hardware; and
- Management GUI software; and
- TOE guidance.

Figure 1-1- Physical Scope of the TOE



1.5.1.2. TOE Software

Check Point VSX and Check Point Provider-1 are software products produced by Check Point. The products are each installed on a hardware platform in combination with an operating system (OS), in accordance with TOE guidance.

The software is shipped to the consumer in a single package containing CD-ROMs with the installation media and user documentation. The package also contains the management GUI software that is included in the TOE.

Figure 1-2 – Check Point VSX Software and Guidance Distribution

As part of its evaluated flaw remediation procedures, Check Point electronically distributes hot fix accumulators (HFAs). There is no HFA included in the TOE.

1.5.1.3. TOE Hardware Platforms

The consumer installs Check Point VSX 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 section A.2. Check Point Provider-1 is installed by the consumer on platforms identified in section A.3.

Figure 1-3 - Check Point VSX-1 9070 Appliance

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

©2012 Check Point Software Technologies Ltd. All Rights Reserved.

Classification: [Unrestricted]—For everyone

software. A hardware clock/timer with on-board battery backup supports the operating system in maintaining reliable timekeeping.

1.5.1.4. TOE Operating Systems

In addition to the software, an operating system (OS) is installed on each hardware platform. The OS supports the TOE by providing storage for audit trail and IDS System data, an IP stack for in-TOE routing, NIC drivers and an execution environment for management daemons.

The software, OS and hardware platform are collectively identified in this ST as the 'Check Point VSX gateway' or ‘Check Point Provider-1 host’.

Product CD-ROMs contains a Check Point proprietary OS identified as Check Point SecurePlatform, a stripped-down version of the Linux operating system. This OS is used on the Check Point Provider-1 host. Check Point VSX gateways run a SecurePlatform variant with virtualization support, Check Point SecurePlatform VSX.

1.5.1.5. TOE Management Architecture

One or more gateways are managed by a Check Point Provider-1 installation that maintains security policy information for the gateways, and collects audit records from the gateways for review by TOE administrators. A Provider-1 installation consists of one or more Check Point Provider-1 hosts. Multiple Provider-1 hosts may be used in a single installation for scalability and fault tolerance.

As described in the TOE evaluated configuration guidance, the Check Point Provider-1 host must be installed on a protected LAN that is directly connected to a TOE Check Point VSX gateway. The gateway protects the Provider-1 host from any direct network access by untrusted entities. The Provider-1 host may manage this gateway, as well as other remote Check Point VSX gateways. It may also manage other Check Point products that are not part of the TOE, such as Check Point Security Gateway appliances. Administrators connect to the Check Point Provider-1 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 protected management LAN; or
- *Remote administration*: a management GUI is installed on a protected LAN that is directly connected to a remote TOE Check Point VSX 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.

©2012 Check Point Software Technologies Ltd. All Rights Reserved.

Classification: [Unrestricted]—For everyone

Figure 1-4 - Local administration of the TOE

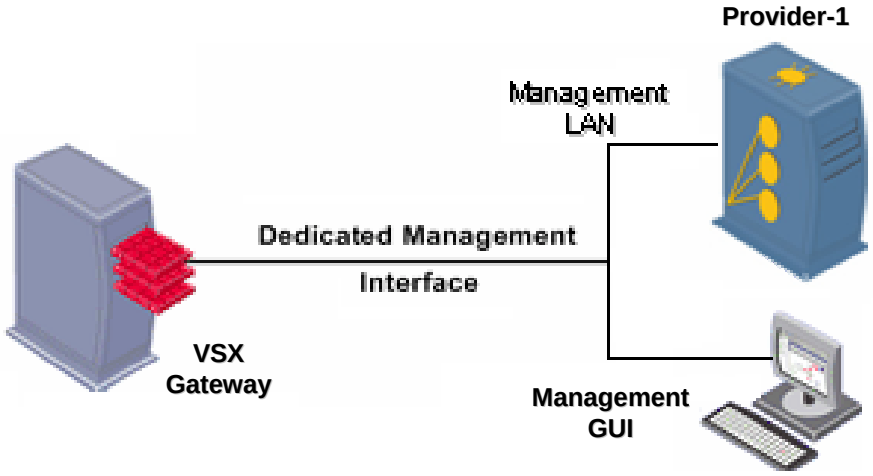
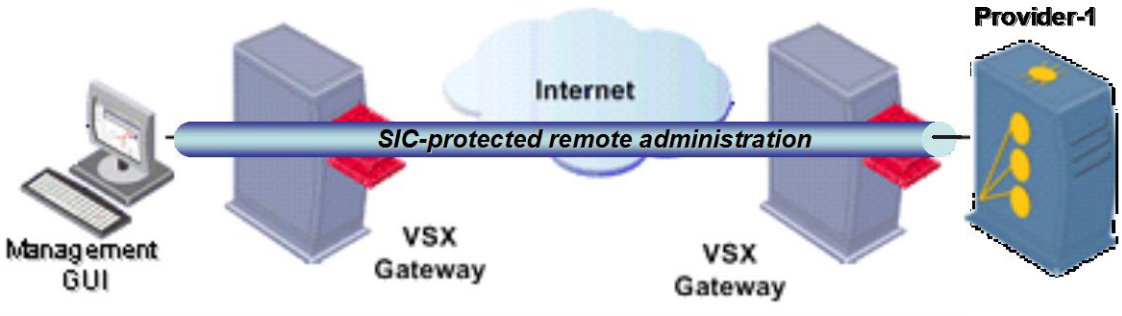


Figure 1-5 - Remote administration of the TOE



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 Check Point VSX gateway. 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: Administration sessions are protected using the Secure Internal Communications (SIC) security function, which incorporates the TLSv1.0 protocol using the FIPS-approved AES encryption algorithm for all communications between management GUIs and Provider-1.

1.5.1.6. VSX Cluster Configurations

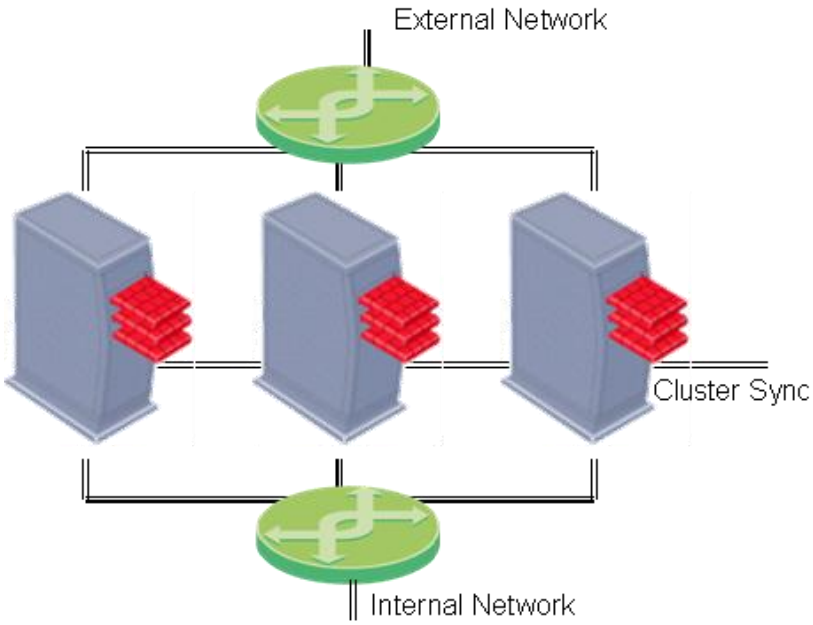
In a VSX cluster configuration, the Check Point VSX gateway is in fact two or more machines installed in parallel. A cluster provides identical functionality to a single gateway, but can provide enhanced performance and fault tolerance. Cluster members are all attached identically to internal and external networks; in addition, each member is

©2012 Check Point Software Technologies Ltd. All Rights Reserved.

Classification: [Unrestricted]—For everyone

attached to one or more dedicated cluster synchronization networks that are isolated by the gateways from any external access.

Figure 1-6 – VSX Cluster Configuration



1.5.1.7. Components in the Operational Environment

The TOE enforces network traffic information flow policies on traffic flowing through Check Point VSX gateways. The TOE relies on the IT environment to route all controlled network traffic flows through the gateways.

The TOE does **not** include the following components that may interact with the TOE, depicted in Figure 1-1 outside the boundaries of the TOE:

- Management GUI hardware and operating system (see section 1.4.3 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 or separately-managed VSX installations for the establishment of secure VPN channels using the IKE/IPSec protocols.
- IPSec VPN and SSL VPN clients.

©2012 Check Point Software Technologies Ltd. All Rights Reserved.

Classification: [Unrestricted]—For everyone

Note: Although the TOE CD-ROM package described below includes other Check Point products that may interact with the TOE such as Check Point Security Gateway and Endpoint Connect (VPN client application), this software is licensed separately and is not considered part of the TOE.

1.5.2. TOE Guidance

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

Table 1-2 - TOE Guidance

Title	Version	Date	Part No.
Common Criteria Guidance			
VSX CC Evaluated Configuration Installation Guide		February 2012	
VSX CC Evaluated Configuration Administration Guide		May 2012	
Administration Guides			
Provider-1	R71	April 6, 2010	
Security Management Server	R71	April 22, 2010	
SmartView Monitor	R71	April 6, 2010	
Check Point IPS	R71	April 6, 2010	
SecurePlatform R71 Admin Guide	R71	April 22, 2010	
Firewall R71 Admin Guide	R71	April 22, 2010	
VPN R71 Admin Guide	R71	December 22, 2010	
ClusterXL R71 Admin Guide	R71	July 31, 2011	

©2012 Check Point Software Technologies Ltd. All Rights Reserved.

Classification: [Unrestricted]—For everyone

1.5.3. Logical Scope of the TOE

1.5.3.1. Summary of TOE Security Functionality

Check Point VSX is a virtualization environment for the implementation of network traffic information flow controls, providing controlled connectivity between two or more network environments. VSX gateway network interfaces are associated with Virtual Systems. Virtual Systems run information flow control programs coded in Check Point's patented INSPECT language. Each Virtual System runs in a separate execution domain, and can read and write packets only from its associated interfaces. Administrator-defined conditional access controls constrain inter-System traffic.

The product 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 administrators have the authority to change the security policy rules.

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

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

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

User authentication may be achieved by a remote access client authenticating using IKE or TLS, against public key credentials held by the user. Administrators also need to authenticate to the TOE before they can use the Management GUIs to access Provider-1. The TOE can be optionally configured to perform user authentication with the support of external authentication servers in the IT environment.

TOE administration is also virtualized. A single Check Point Provider-1 installation can support many Customer management domains. A separate management database is maintained for each Customer, providing separation of security management data and audit logs between domains.

Administrators can perform both local and remote management of the TOE. AES encryption is used to protect remote management sessions. Administrator sessions are protected via a trusted path between the management GUI and Provider-1. Internal TOE communications between Check Point Provider-1 hosts and Check Point VSX gateways is also protected from disclosure and undetected modification.

©2012 Check Point Software Technologies Ltd. All Rights Reserved.

Classification: [Unrestricted]—For everyone

Audit trail data and IDS System 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 an 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 an 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 VSX gateway protects itself and the Check Point Provider-1 installation 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 VSX gateways and Provider-1 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. Virtual Systems

Check Point VSX is based on Check Point's Security Gateway product. Its goal is to allow administrators to model large numbers of virtual network and security elements using a limited number of gateway platforms.

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 is integrated into the Check Point VSX gateway's operating system kernel. It 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.

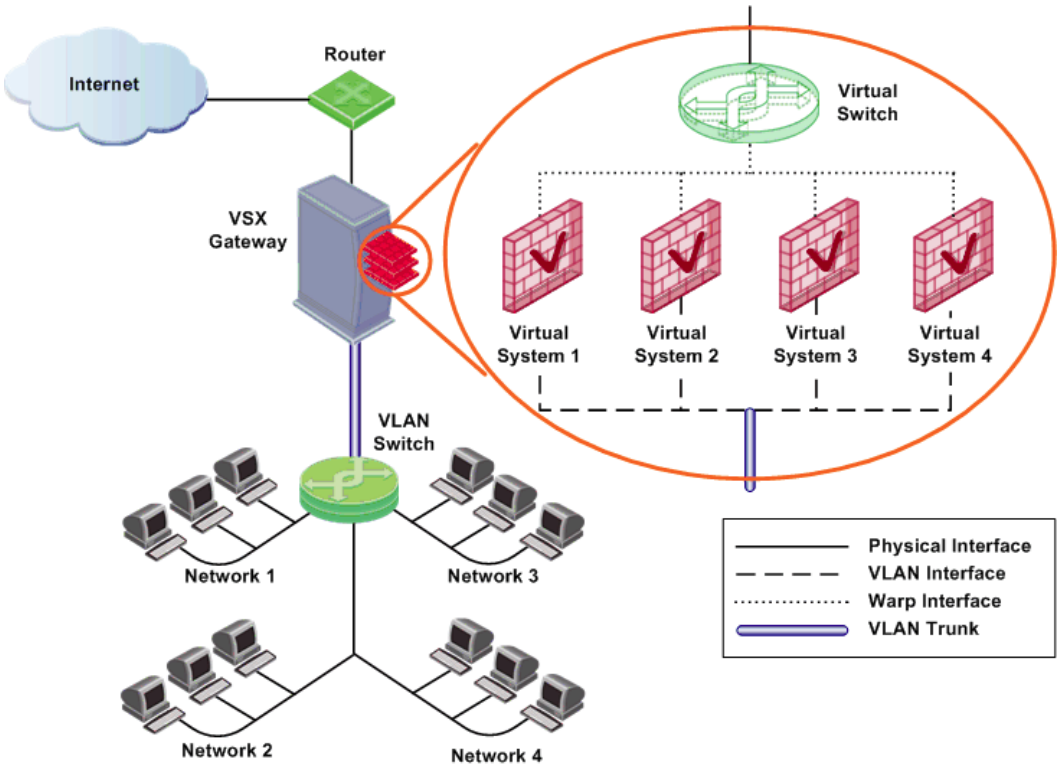
The Virtual System abstraction allows the administrator to model virtually any multi-gateway networking configuration. Supported Virtual System types include:

©2012 Check Point Software Technologies Ltd. All Rights Reserved.

Classification: [Unrestricted]—For everyone

- **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.

Figure 1-7 - Virtualization – a Typical Configuration



1.5.3.3. 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.

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 TOE, which associates them with application-level connections, using the IP packet header fields. Fragmented packets are reassembled before they are processed.

©2012 Check Point Software Technologies Ltd. All Rights Reserved.

Classification: [Unrestricted]—For everyone

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

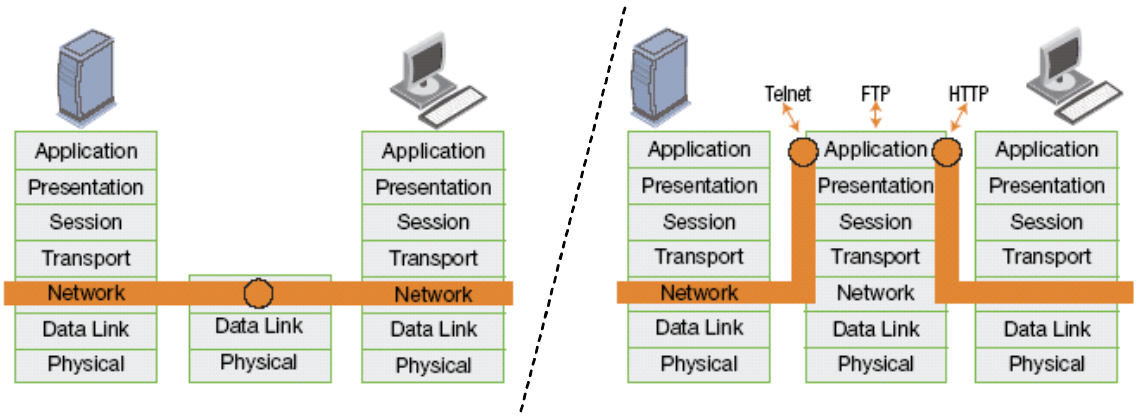
Network Address Translation (NAT) rules can modify source and/or destination addresses and/or UDP or TCP ports according to administrator-defined policies, supporting configurations where communicating end points do not interact with the actual IP address of their peers.

1.5.3.4. 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 1-8- Traffic filtering (left) vs. Application-level Proxies



Check Point VSX uses Stateful Inspection to provide the best of both architectures. 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 System 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

©2012 Check Point Software Technologies Ltd. All Rights Reserved.

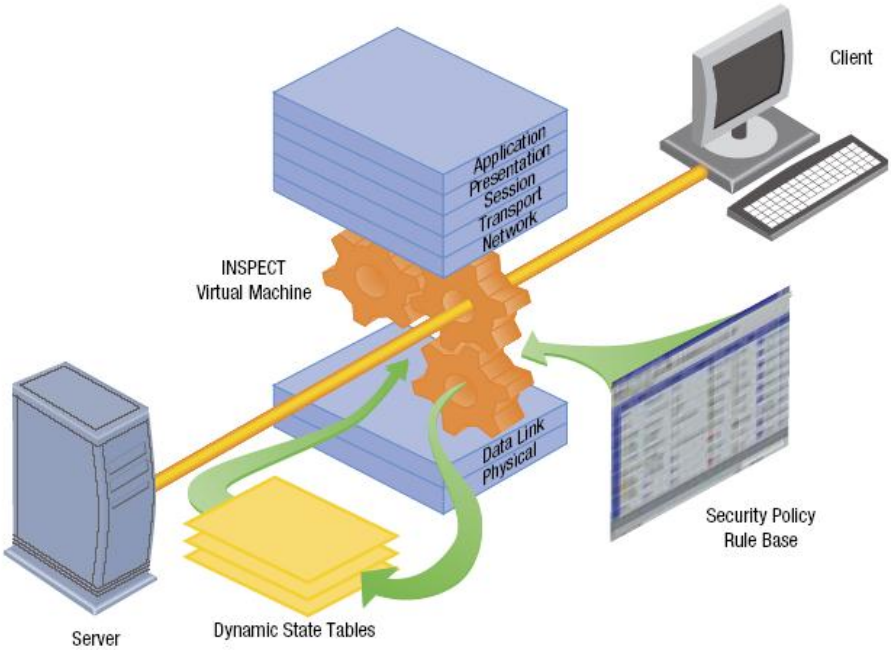
Classification: [Unrestricted]—For everyone

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 the Check Point VSX gateway as a kernel-level virtual machine. Security policy is compiled on Check Point Provider-1 into virtual machine inspection code that is downloaded to the gateway. The inspection code operates on incoming packets before they even reach the operating system IP stack.

Figure 1-9 - Stateful Inspection



The TOE's traffic filtering and IDS/IPS capabilities are based on the INSPECT engine. Traffic filtering matches traffic headers with an ordered set of administrator-defined rules in the Security Rule Base rules, which allow, drop, or reject (notifying the traffic source) incoming packets. 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 logging level.

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

©2012 Check Point Software Technologies Ltd. All Rights Reserved.

Classification: [Unrestricted]—For everyone

Figure 1-10- Example Rule

1.5.3.5. Intrusion Detection/Prevention

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

IDS signatures may be defined manually by the administrator, or downloaded from a Check Point 'SmartDefense Update' subscription service. Signature updates are installed as INSPECT code fragments (see section 1.5.3.4 above), and are packaged with corresponding GUI updates to integrate seamlessly with previously installed defenses.

1.5.3.6. Virtual Private Networking (VPN)

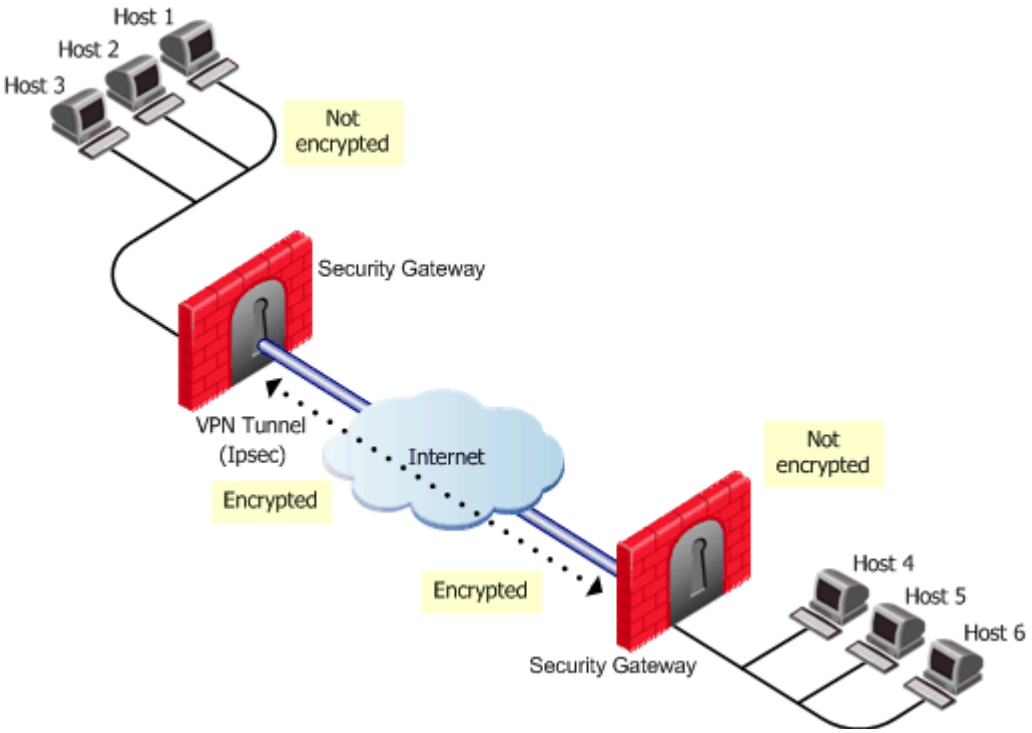
A VPN provides the ability to use a public or untrusted network, such as the Internet, as if it were a secure, private network. A VPN is created through the use of devices that can establish secure communication channels over a common communications infrastructure, protecting data in-transit between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

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

©2012 Check Point Software Technologies Ltd. All Rights Reserved.

Classification: [Unrestricted]—For everyone

Figure 1-11- Virtual Private Network



A Check Point VSX 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.

©2012 Check Point Software Technologies Ltd. All Rights Reserved.

Classification: [Unrestricted]—For everyone

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.

1.5.3.7. 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 System 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.

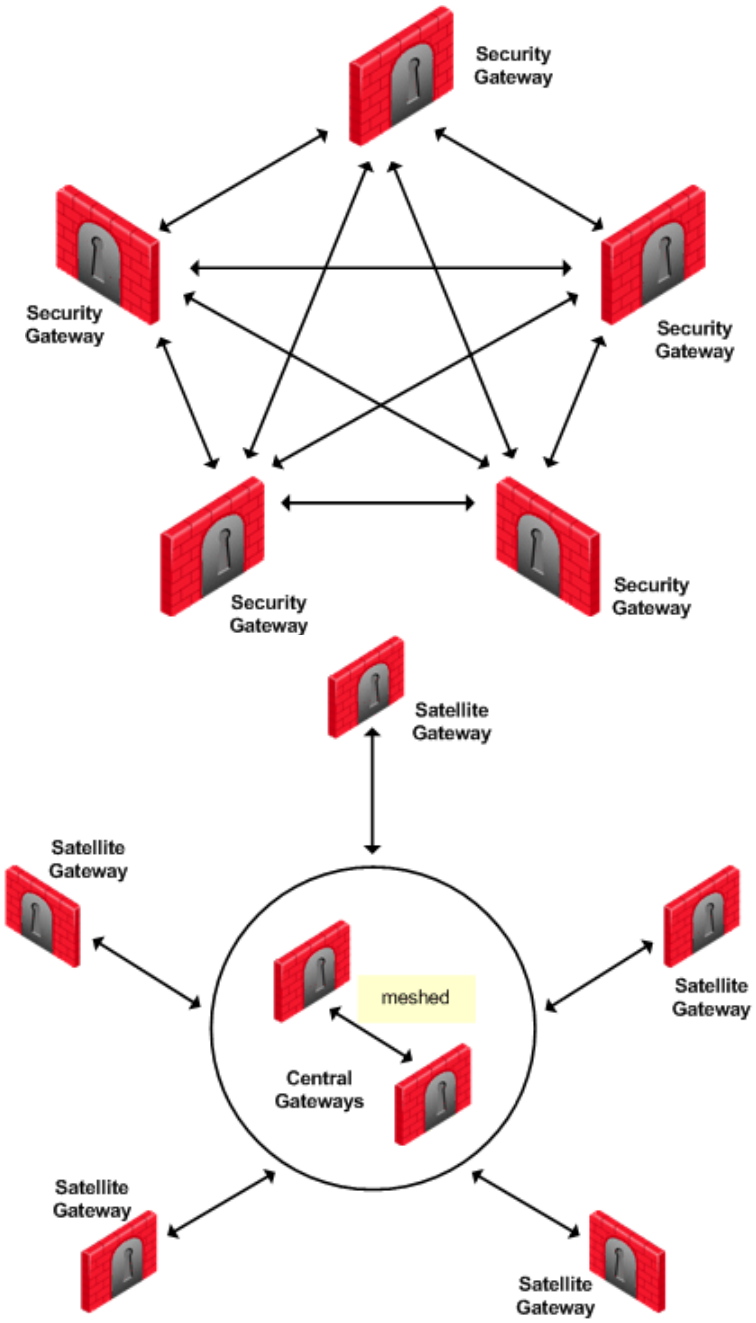
VPN community topologies may be combined (e.g. a star where each satellite is a meshed community). Complex VPN architectures can be defined without having to resort to manually defining each VPN tunnel created between any two gateways.

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

Figure 1-12 – Remote Access VPN Client Software running on a PDA

©2012 Check Point Software Technologies Ltd. All Rights Reserved.
Classification: [Unrestricted]—For everyone

Figure 1-13- 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 System 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.

©2012 Check Point Software Technologies Ltd. All Rights Reserved.

Classification: [Unrestricted]—For everyone

In the example given in Figure 1-14 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 1-14- VPN community used as a Rule Base security attribute

1.5.3.8. Extended VPN Capabilities

Check Point VSX gateways 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 VSX supports a hybrid mode for remote access clients where the gateway authenticates using a certificate, and the client authenticates using password that can be authenticated with the help of an authentication server in the IT environment.

Multiple Entry Points (MEP) - Check Point VSX gateways 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 clients – 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.

©2012 Check Point Software Technologies Ltd. All Rights Reserved.

Classification: [Unrestricted]—For everyone

1.5.3.9. 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 Check Point Provider-1 installation, and accessed by administrators using management GUIs. Provider-1 distributes network configuration and security policy information to Check Point VSX gateways, and collects audit records for storage and review.

Provider-1 maintains separate Customer management domains. Each Virtual System is associated with a single Customer domain. All Customer-specific information, including Virtual System configuration, Customer security policies and Customer audit records are stored in separate databases for each Customer.

Management interfaces include Provider-1 Multi-Domain GUI (MDG) and SmartConsole. SmartConsole is an integrated set of management GUI applications, including SmartDashboard, SmartView Tracker, and SmartView Monitor.

The MDG allows an administrator to manage the Provider-1 installation, including definition and monitoring of Provider-1 hosts, high-availability, Customers, management GUI hosts, and administrator accounts. The SmartConsole applications allow an administrator to administer the TOE security policy, review audit trail and IDS System data, and monitor gateway status.

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.

1.5.3.10. Administrator Roles

When an administrator connects to the Provider-1 installation using a management GUI, he or she specifies a target management domain. MDG always connects to a Provider-1 *Multi-Domain Server* (MDS) domain, which maintains global TSF data that pertains to the Provider-1 installation itself. SmartConsole users connect to a *Customer Management Add-on* (CMA) installed on a MDS container. The CMA maintains only Customer-specific TSF data, for a single Customer domain. Many Virtual Systems may be managed by a single CMA.

SmartDashboard can also connect to the MDS, in order to manage global security, IDS/IPS and VPN policies that can be applied to multiple CMAs, combined with the corresponding per-CMA defined policy. In this mode, the application is labeled 'Global SmartDashboard'. MDS-level audit trails can be reviewed by connecting to the MDS using SmartView Tracker.

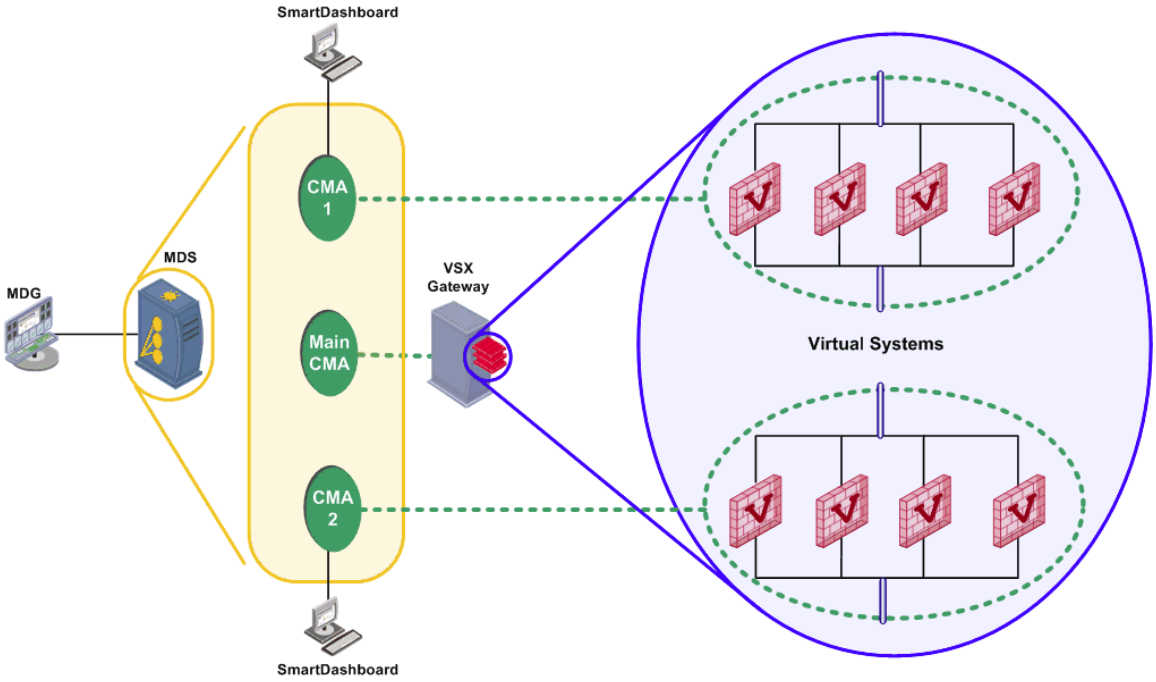
The TOE associates administrator accounts with granular permissions, providing control of both the functions that the administrator may access, and the scope of control (i.e. which Customers the administrator may access). In this ST, management roles are defined in terms of management scope: a MDG or Global SmartDashboard administrator connecting to the MDS is considered to be in an *authorized administrator* role; an

©2012 Check Point Software Technologies Ltd. All Rights Reserved.

Classification: [Unrestricted]—For everyone

administrator using the SmartConsole applications is considered to be in an *authorized System administrator* role.

Figure 1-15 - Provider-1 VSX Management Model



1.5.3.11. Internal Certificate Authority (ICA)

Check Point Provider-1 contains an internal certificate authority component (ICA) that manages certificates used for securing management traffic between a Provider-1 installation and managed Check Point VSX gateways. The ICA publishes CRLs internally to TOE components. The ICA also generates administrator certificates for authenticating management GUI users. In addition to the main ICA maintained by the Provider-1 installation, a separate ICA is used for each Customer, to manage certificates used for securing internal communications between the Customer domain and its Virtual Systems.

All internal communications between distributed TOE components (except for the cluster synchronization traffic as described in section 1.5.1.6), as well as communications with remote trusted IT entities that interact with the TOE using OPSEC APIs (see below), are protected using a Secure Internal Communications (SIC) mechanism that incorporates the TLSv1.0 protocol, using AES encryption. Certificates for SIC are generated and managed by an Internal Certificate Authority (ICA).

ICA can also be used to generate certificates for VPN gateways and for external users; however, the evaluated configuration rule base does not allow external access to the Provider-1 installation, so that certificate management for external users in the evaluated configuration must be performed in an offline manner.

©2012 Check Point Software Technologies Ltd. All Rights Reserved.

Classification: [Unrestricted]—For everyone

1.5.3.12. OPSEC Client APIs

Provider-1 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 IT entity account.

1.5.3.13. Fault Tolerance

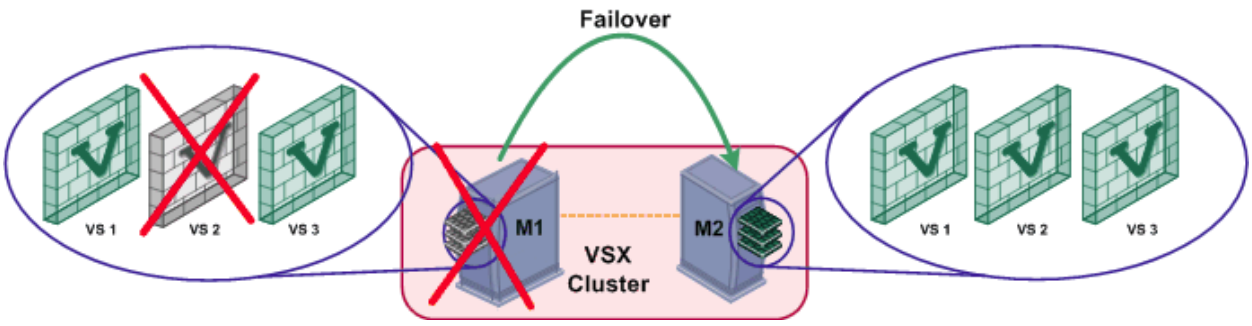
Fault tolerance is ensured through redundancy. Multiple Provider-1 hosts and VSX gateways ensure that when a failure is detected on an active host or gateway, the TOE can transfer control to a standby host or gateway.

Multiple Provider-1 hosts synchronize MDS and CMA databases between themselves. If a host fails, administrators can transition standby MDSs and CMAs installed on other hosts to an active status, and continue management operations.

Security policy is installed on all cluster members, and state information is synchronized over dedicated synchronization interfaces, allowing the TOE to transfer information flow control processing between cluster members without connection loss.

- **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.

Figure 1-16 - VSX Gateway High Availability



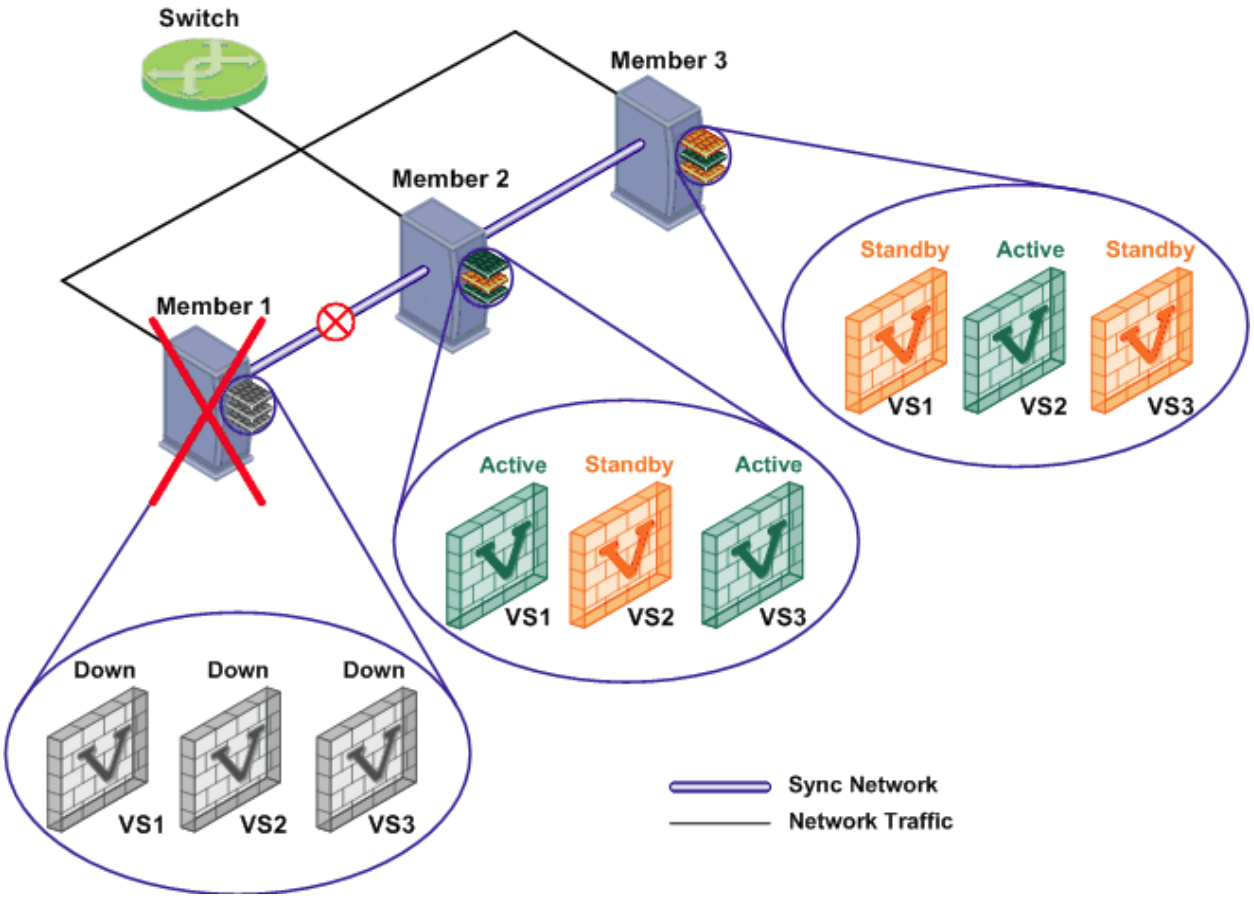
©2012 Check Point Software Technologies Ltd. All Rights Reserved.

Classification: [Unrestricted]—For everyone

- **Virtual System Load Sharing (VSLS)** – in this mode, the VSX cluster automatically distributes Virtual Systems among all operational cluster members, in accordance with administrator-defined Virtual System priorities and weights. A Virtual System on a cluster member may be in one of the following states:
  - **Active** – the Virtual System is processing information flow control requests and updating state tables.
  - **Standby** – the Virtual System is receiving state synchronization updates from the Active Virtual System.
  - **Backup** – the Virtual System maintains the up-to-date security policy information, but does not receive state synchronization updates.

Figure 1-17 below depicts a failure scenario where an active Virtual System fails on one member, but the standby and backup Virtual Systems remain up. In this case, the active Virtual System fails over to its standby peer (in this case on Member 2) and its backup (on member 3) becomes the standby, synchronizing with the new active member.

Figure 1-17 - Virtual System Load Sharing (VSLS)



©2012 Check Point Software Technologies Ltd. All Rights Reserved.

Classification: [Unrestricted]—For everyone

1.5.3.14. Time Synchronization

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

The evaluated configuration guidance instructs the administrator to configure this interaction such that the NTP server is authenticated using an MD5 shared secret.

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 Provider-1, with an indication of the originating component and the local time stamp. In addition, log files from each appliance are periodically forwarded to Provider-1, and can be reviewed individually.

1.5.3.15. Functionality Excluded from the TOE Evaluated Configuration

The Check Point VSX product can provide a broad range of services (product types), features and capabilities. Some of these require additional products or licenses to be installed on the Check Point VSX gateway and/or on the Check Point Provider-1 host.

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:

- **SNMP daemon** – Check Point VSX gateways provide optional SNMP daemons that can be used for remote management. These daemons are not available when the TOE is in FIPS mode.
- **CLIs and SSH** - Check Point VSX gateways 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 Check Point Provider-1 hosts. The CLI can be accessed from a directly connected console or remotely using the SSH protocol.

  In the evaluated configuration, these CLIs should not be used after this installation stage. All management of the TOE should be performed via the management GUIs. If a VSX gateway must be reconfigured (e.g. a NIC is physically added to the appliance), it should be reinstalled to ensure that it remains in a secure configuration.
- **LDAP User Management** – the TOE supports the LDAP protocol for managing users on an external LDAP directory server. LDAP User Management requires an additional SmartDirectory license to be installed. User authentication and authorization information is retrieved from the directory over a se-

©2012 Check Point Software Technologies Ltd. All Rights Reserved.

Classification: [Unrestricted]—For everyone

cure channel. This configuration is not being evaluated and is outside the TOE evaluated configuration.

- **Dynamic Routing** - Check Point VSX gateways 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.
- **Bridge Mode** – Check Point VSX enables configuration of Virtual Systems in Bridge Mode, each bridging two network interfaces. Bridged network frames (containing IP packets) are forwarded after processing the packet as for routed packets. However, Virtual Systems in Bridge Mode do not support all claimed security functionality (in particular, VPN and NAT are not supported), and therefore are not included in the evaluated configuration.
- **Content Inspection** –Check Point VSX allows the administrator to enable a URL filtering component on the appliance itself, given an appropriate Content Inspection license. Evaluated configuration guidance instructs administrators not to enable this functionality.

©2012 Check Point Software Technologies Ltd. All Rights Reserved.

Classification: [Unrestricted]—For everyone

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 sk66142 provides resources related to this evaluation. 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 VSX 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

©2012 Check Point Software Technologies Ltd. All Rights Reserved.

Classification: [Unrestricted]—For everyone

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

1.5.4.6. SmartDefense Services

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

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

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

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

©2012 Check Point Software Technologies Ltd. All Rights Reserved.

Classification: [Unrestricted]—For everyone

1.5.5. Example Deployment Strategies

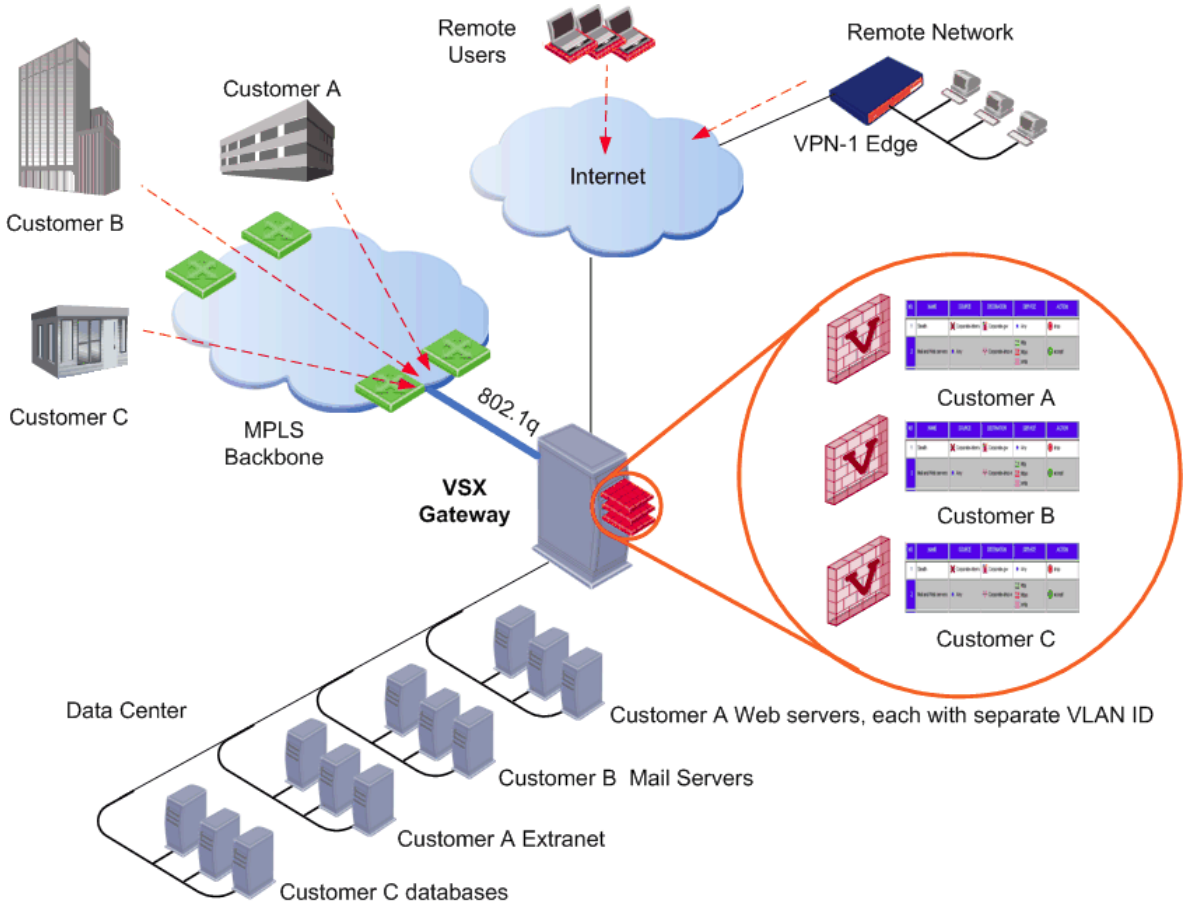
The following subsections provide some examples for VSX and Provider-1 deployment strategies, in order to help the reader gain a general understanding of the TOE's intended IT environment and its logical security features.

1.5.5.1. Data Centers

Data center providers supply external hosting services for customer servers and databases. The service typically includes infrastructure, connectivity, and security for multiple customers. The example scenario presented in Figure 1-18 shows multiple customer networks sharing a common physical infrastructure and MPLS backbone that provide connectivity between each customer and the data center.

Customer A connects to its web hosting servers. Customer B connects to its mail servers, and Customer C connects to its database servers. To provide network security and management, the data center provider deploys a VSX gateway with separate Virtual Systems for each customer. Each customer can deploy independent firewall, IDS/IPS, and VPN security controls, and manage them remotely from his premises, using a centralized Provider-1 installation located in the data center.

Figure 1-18 - Data Center Deployment



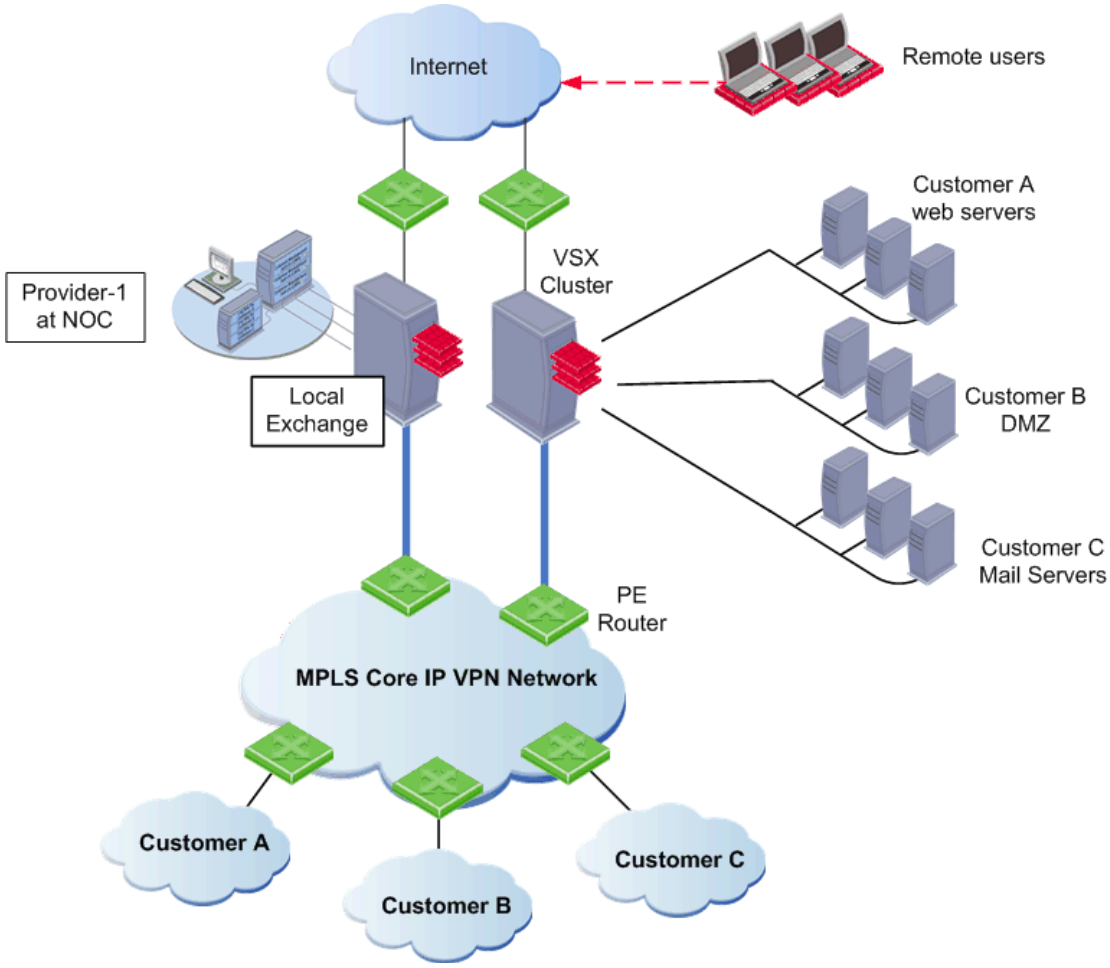
©2012 Check Point Software Technologies Ltd. All Rights Reserved.
Classification: [Unrestricted]—For everyone

1.5.5.2. Managed Security Provider (MSP)

Managed service providers supply connectivity and security services for customer networks. Some of these customers require remote access capabilities. In this service oriented environment, VSX and Provider-1 provide central management while facilitating connectivity and security without affecting the existing IP topology.

In the example shown in Figure 1-19, a VSX cluster resides in a Point of Presence (POP) deployment for a service provider. VSX consolidates hardware for the service provider while ensuring privacy and secure connectivity solutions (VPN) for customers. VSX and Provider-1 provide a centralized, granular provisioning system, where each customer manages its own security without the ability to define Virtual Systems and other network components

Figure 1-19 - MSP Deployment



©2012 Check Point Software Technologies Ltd. All Rights Reserved.

Classification: [Unrestricted]—For everyone

1.5.5.3. Enterprise Deployment

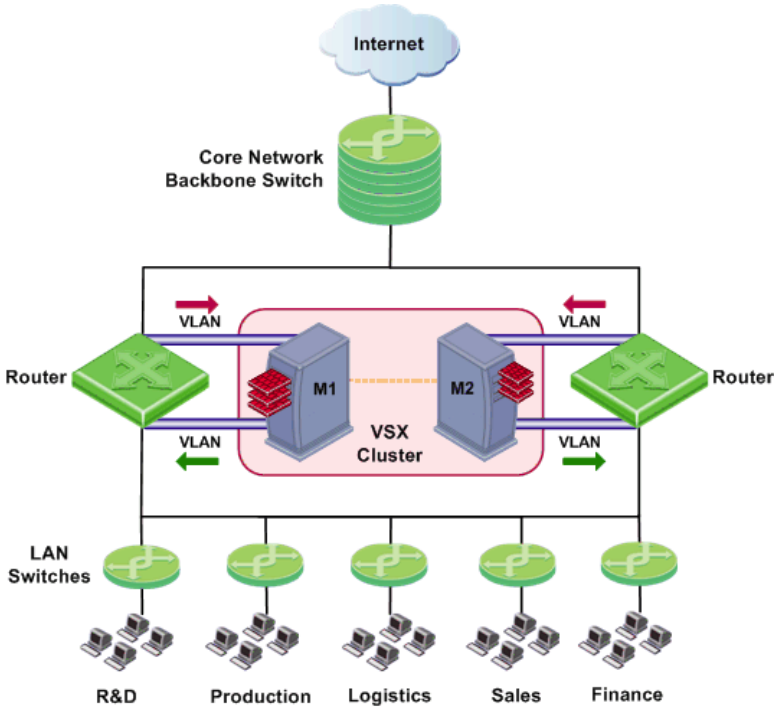
A common Enterprise network architecture, appropriate for large, high-traffic network environments, consists of three networking layers:

1. **Core network** - comprised of high-speed backbone switches directs traffic between corporate sites, and to and from the Internet and other external networks.
2. **Distribution layer** - comprised of routers, provides connectivity between the core and the access layer.
3. **Access layer** - comprised of redundant LAN switches, forwards traffic to and from internal networks.

A Check Point VSX cluster can be incorporated into the distribution layer, as depicted below in Figure 1-20. The VSX gateways mediate traffic flowing in and out of the access layer switches.

Separate Virtual Systems can be deployed to protect different divisions or departments, each applying its own independently managed security policy. Multiple Provider-1 Customer management domains can be used to segregate security management. For example, Corporate Finance might be defined as a Customer; administrators assigned an authorized System administrator role for Corporate Finance would be able to manage Corporate Finance Virtual Systems across the distributed enterprise, but would not be able to access security management information for other divisions.

Figure 1-20 - Three Layer Hierarchical Model



©2012 Check Point Software Technologies Ltd. All Rights Reserved.

Classification: [Unrestricted]—For everyone

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 3, July 2009, CCMB-2009-07-002, extended (CC Part 2 Extended)
- Common Criteria for Information Technology Security Evaluation Part 3: Security assurance requirements, Version 3.1 Revision 3, July 2009, CCMB-2009-07-003, 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 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] and [IDSSPP], both CCv3.1 PPs that require demonstrable PP conformance.

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:

- All threats and OSPs defined in all claimed PPs are redefined in identical form in sections 3.1 and 3.3, respectively. Section 3.1.4 and 3.1.5 define additional threats that are countered by the TOE's Virtualization, VPN, and fault tolerance functionality. In relation to any of the individual claimed PPs, the definition of

©2012 Check Point Software Technologies Ltd. All Rights Reserved.

Classification: [Unrestricted]—For everyone

additional threats and OSPs serves to make the security problem definition more restrictive, and cannot cause inconsistency in of itself.

- This ST omits most of the assumptions defined in the claimed PPs. The omission of an assumption makes the security problem definition more restrictive[10] in that assumptions constrain the required security solution.
- 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 [TFF-PP] A.PHYSEC assumption that "the TOE is physically secure".

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 [TFF-PP] assumptions and is thus consistent with all 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 [TFF-PP].

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 [TFF-PP] security objectives, with the qualifications specified in section 4.1.1. Appropriate [IDSSPP] objectives were then restated, except for objectives identified in section 4.1.2 that were determined to be either substantially equivalent to corresponding [TFF-PP] objectives (with the equivalency identified in subsection 2.4.3.1), or irrelevant in the context of this ST.

Subsection 2.4.3.2 below demonstrates the consistency of the security objectives for the environment in this ST in relation to the claimed PPs.

[10] [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.

©2012 Check Point Software Technologies Ltd. All Rights Reserved.

Classification: [Unrestricted]—For everyone

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; only sensing.	The [IDSSPP] requires that a conformant TOE must include at least one Sensor or Scanner (see [IDSSPP] application note for IDS_SDC.1), but does not require both. The Check Point VSX 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

©2012 Check Point Software Technologies Ltd. All Rights Reserved.

Classification: [Unrestricted]—For everyone

[IDSSPP] objective	Equivalent in this ST	Omission rationale
		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 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[11] 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[12].

Table 2-2 - PP Conformance and Environment Security Objectives

Objective	[TFF-PP]	[IDSSPP]
NOE.INSTALL	Equivalent to O.GUIDANCE	Identical to OE.INSTAL

[11] 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.

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

©2012 Check Point Software Technologies Ltd. All Rights Reserved.

Classification: [Unrestricted]—For everyone

Objective	[TFF-PP]	[IDSSPP]
NOE.ADMTRA	Restrictive integration of the [TFF-PP] O.ADMTRA[13] with the [IDSSPP] OE.PERSON.	
NOE.PHYSICAL	Equivalent to A.PHYSEC	Equivalent to OE.PHYCAL
NOE.CREDEN	While not explicitly stated in [TFF-PP], it should be applicable to that PP 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 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 objectives and requirements of both [TFF-PP] and [IDSSPP], except for the FIA_AFL.1 and FIA_SOS.1 requirements that are inapplicable to the TOE (see rationale below).

All security requirements from all claimed 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.

[13] Note that the NOE.ADMTRA is also consistent with [TFF-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.

©2012 Check Point Software Technologies Ltd. All Rights Reserved.

Classification: [Unrestricted]—For everyone

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 'basic' level of audit is appropriate for all claimed PPs. The assignment of *other specifically defined auditable events* made in [IDSSPP]: "**Access to the System and access to the TOE and System data**" is specified by the FAU_GEN.1 entries in Table 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.

The entry for FPT_STM.1 as an auditable event given in [TFF-PP] has been omitted from this ST. FMT_MOF.1 has 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 refined (in relation to the claimed PPs) to conform with CCv3.1 Part 2 syntax, inclusive of the corresponding requirements in [TFF-PP], [IDSSPP]. Specifically, [TFF-PP] requires searches and sorting, the [IDSSPP] requires only sorting, [TFF-PP] requires b) through e), [IDSSPP] requires a), c), d), f) and g). Highlighting is presented in relation to the original CCv3.1 Part 2 requirement.

2.4.4.4. FAU_SEL.1

FAU_SEL.1 is as stated in [IDSSPP].

This requirement is inclusive of the corresponding requirements in [IDSSPP]. Specifically, [IDSSPP] requires audit selectivity based on event type.

2.4.4.5. FAU_STG.2

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

©2012 Check Point Software Technologies Ltd. All Rights Reserved.

Classification: [Unrestricted]—For everyone

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

2.4.4.6. FAU_STG.4

FAU_STG.4 has been derived from all claimed PPs.

FAU_STG.4 has been refined in relation to all claimed PPs in order to be inclusive of the corresponding requirement in each of the PPs. The term ‘prevent’ is taken from [TFF-PP]; The [IDSSPP] allow other options (e.g. overwriting the oldest stored audit records) as well. Sending an alarm is a requirement in [IDSSPP]. Limiting the number of audit records lost (and providing an analysis thereof – see Table 7-1) is a requirement in [TFF-PP].

2.4.4.7. FCS_COP.1 /Admin

FCS_COP.1 /Admin is derived 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.

2.4.4.8. FDP_IFC.1 /TFF

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

The original [TFF-PP] UNAUTHENTICATED SFP is refined here to allow traffic filtering for authenticated external IT entities (see also section 6.1.4.2). This is consistent with [TFF-PP] because it is more restrictive.

The original [TFF-PP] syntax is used in FDP_IFC.1 /TFF for enhanced readability and for consistency with the PP, describing information flows as occurring between external IT entities. See FDP_IFC.1 /TFF application note for the interpretation of subjects and information defined for the TRAFFIC FILTER SFP.

2.4.4.9. 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

©2012 Check Point Software Technologies Ltd. All Rights Reserved.

Classification: [Unrestricted]—For everyone

stateful packet inspection (derived from the more-restrictive [PPFWTFMR] Protection Profile), and NAT.

The term "loopback address" in FDP_IFF.1.5 subsection c) 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. FIA_AFL.1

The FIA_AFL.1 requirement appearing in [TFF-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.

2.4.4.11. FIA_ATD.1

FIA_ATD.1 has been derived from all claimed PPs.

The [IDSSPP] notation was used for FIA_ATD.1. The [IDSSPP] user is an administrator; therefore, authorisations refer to administrator authorisations. [TFF-PP] defines only two attributes: identity; mapped here to user identity, and association of a human user with the authorized administrator role. The latter attribute corresponds here to a non-empty set of authorisations.

2.4.4.12. FIA_UAU.1

FIA_UAU.1 is as stated in [IDSSPP] and refined in relation to [TFF-PP].

The [IDSSPP] FIA_UAU.1 component requires the ST to define any mediated actions that permitted before a user is authenticated. [TFF-PP] restricts administrator and authorized IT entity actions before authentication to user identification. The unauthenticated actions identified in FIA_UAU.1.1 subsections a) through d) are all unauthenticated actions performed by external IT entities, in support of subsequently performing authentication in accordance with FIA_UAU.5, and are therefore compatible with [TFF-PP]. In addition, [TFF-PP] clearly allows unauthenticated information flows; subsection e) is therefore also considered to be consistent with intent of this PP.

2.4.4.13. FIA_UID.2

FIA_UID.2, specified in [TFF-PP], is hierarchical to the FIA_UID.1 component specified in [IDSSPP].

©2012 Check Point Software Technologies Ltd. All Rights Reserved.

Classification: [Unrestricted]—For everyone

2.4.4.14. FMT_MOF.1

FMT_MOF.1 is derived from [TFF-PP], which defines it as the sole FMT class SFR, restricting all security management functions to the [TFF-PP] authorized administrator role, and allowing the ST author to specify additional security-relevant administrative functions.

All [TFF-PP] FMT_MOF.1 subsections have been restated in FMT_SMF.1 Table 6-3, and FMT_MOF.1 refined to refer to that table. In addition, the single [TFF-PP] authorized administrator role has been refined here to be consistent with the more granular approach implemented by the TOE.

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.

2.4.4.15. FMT_MTD.1

FMT_MTD.1 been derived from [IDSSPP].

FMT_MTD.1 is refined in relation to [IDSSPP] 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.

2.4.4.16. 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] define a single ‘authorized administrator’ role that is mapped in this ST to the following roles identified in FMT_SMR.1: authorized administrator and authorized System administrator. The [TFF-PP] FMT_SMR.1 requirement is refined to be consistent with CCv3.1 syntax and with the other PPs; its requirement that the authorized administrator role must be associated only with human users (and not with trusted external IT entities) is instead adequately expressed by the FIA_USB.1 /Admin component in this ST

©2012 Check Point Software Technologies Ltd. All Rights Reserved.

Classification: [Unrestricted]—For everyone

2.4.4.17. 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”.

2.4.4.18. 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]	FDP_IFF.1	The term "loopback address" is to be used in place of "loopback network"
[PD-0055]	[TFF-PP], [IDSSPP]	Objectives for the environment	Additional assumptions are allowed if they do not violate the intent of the PP
[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]	[TFF-PP]	FIA_UAU.5	IKE authentication is acceptable as "single use"
[PD-0115]	[TFF-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

Both [TFF-PP] and [IDSSPP] require 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.

©2012 Check Point Software Technologies Ltd. All Rights Reserved.

Classification: [Unrestricted]—For everyone

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 and IDS PPs, as well as threats that are countered by the TOE's Virtualization, VPN, and fault tolerance functionality.

3.1.1. Firewall-related Threats

The following threats are identified in [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 bypass 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.AUMACC	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.

©2012 Check Point Software Technologies Ltd. All Rights Reserved.

Classification: [Unrestricted]—For everyone

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.

©2012 Check Point Software Technologies Ltd. All Rights Reserved.

Classification: [Unrestricted]—For everyone

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 Customer data flowing through or stored within the TOE.

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] 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.

©2012 Check Point Software Technologies Ltd. All Rights Reserved.

Classification: [Unrestricted]—For everyone

3.3. Organizational Security Policies

3.3.1. Virtualization OSPs

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

P.CUST The TOE shall enforce separation between Customer networks and data and allow controlled sharing of information.

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.

©2012 Check Point Software Technologies Ltd. All Rights Reserved.

Classification: [Unrestricted]—For everyone

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 Virtualization, 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 [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.

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.
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 from users on a connected network to users on another connected network, and must ensure 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[14] 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.

[14] In contrast with [IDSSPP], the [TFF-PP] defines a single administrator role: ‘authorized administrator’. Therefore, the [TFF-PP]-derived security objectives referring to the authorized administrator should be interpreted as referring to any authorized administrator role, rather than to the specific ‘authorized administrator’ role in FMT_SMR.1.

©2012 Check Point Software Technologies Ltd. All Rights Reserved.

Classification: [Unrestricted]—For everyone

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[14] use of security functions related to audit.

O.SECFUN The TOE must provide functionality that enables an authorized administrator[14] to use the TOE security functions, and must ensure that only authorized administrators[14] are able to access such functionality.

O.LIMEXT The TOE must provide the means for an authorized administrator[14] 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. Virtualization Objectives

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

O.CMA Customer data stored within the TOE shall be restricted to administrators authorized for the Customer management domain.

©2012 Check Point Software Technologies Ltd. All Rights Reserved.

Classification: [Unrestricted]—For everyone

4.1.4. 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 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.

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 physical attack which might compromise IT security objectives.

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.

©2012 Check Point Software Technologies Ltd. All Rights Reserved.

Classification: [Unrestricted]—For everyone

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 pro-vide 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, IPSec VPN and SSL VPN clients are 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.

©2012 Check Point Software Technologies Ltd. All Rights Reserved.

Classification: [Unrestricted]—For everyone

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.

©2012 Check Point Software Technologies Ltd. All Rights Reserved.

Classification: [Unrestricted]—For everyone

4.3. Security Objectives Rationale

The [TFF-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, Virtualization, 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 and Table 4-2 each map the security objectives defined in this ST to threats defined in sections 3.1.1 and 3.1.2, respectively, for [TFF-PP] and [IDSSPP]-related threats. Table 4-3 maps security objectives defined in sections 3.1.3, 3.1.4, and 3.1.5 for virtualization, 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[11] to the mapping given in [TFF-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] threats

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

©2012 Check Point Software Technologies Ltd. All Rights Reserved.

Classification: [Unrestricted]—For everyone

	T.NOAUTH	**T.REPEAT**	**T.REPLAY**	**T.ASPOOF**	**T.MEDIAT**	**T.OLDINF**	**T.PROCOM**	**T.AUMACC**	**T.SELPRO**	**T.AUDFUL**	**T.TUSAGE**
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.CMA											
O.VPN											
O.FAULT											
NOE.INSTALL											✓
NOE.ADMTRA											✓
NOE.PHYSICAL											
NOE.CREDEN											
OE.SINGEN											
OE.IDAUTH	✓										
OE.VPN											
OE.VLAN											

©2012 Check Point Software Technologies Ltd. All Rights Reserved.

Classification: [Unrestricted]—For everyone

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], 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] 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].

©2012 Check Point Software Technologies Ltd. All Rights Reserved.

Classification: [Unrestricted]—For everyone

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														
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.CMA														
O.VPN														
O.FAULT														
NOE.INSTALL						✓								
NOE.ADMTRA														
NOE.PHYSICAL														
NOE.CREDEN														
OE.SINGEN														
OE.IDAUTH	✓	✓	✓	✓	✓	✓								
OE.VPN														

©2012 Check Point Software Technologies Ltd. All Rights Reserved.

Classification: [Unrestricted]—For everyone

	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
OE.VLAN														

4.3.1.3. Other Threats Defined in this ST

Table 4-3 -Tracing of security objectives to other threats defined in this ST

	T.ACCESS	T.NACCESS	T.NMODIFY	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.CMA	✓			
O.VPN		✓	✓	
O.FAULT				✓
NOE.INSTALL				
NOE.ADMTRA				
NOE.PHYSICAL				
NOE.CREDEN				
OE.SINGEN				

©2012 Check Point Software Technologies Ltd. All Rights Reserved.

Classification: [Unrestricted]—For everyone

	T.ACCESS	T.NACCESS	T.NMODIFY	T.FAULT
OE.IDAUTH	✓			
OE.VPN		✓	✓	
OE.VLAN	✓			

The description of the TOE security environment introduces four additional threats on top of the PP-defined threats, that are countered by the TOE's virtualization, VPN, and fault-tolerance IT security functionality:

T.ACCESS *An unauthorized person or external IT entity may be able to access Customer data flowing through or stored within the TOE.*

This threat is countered by O.MAC and O.CMA, which require the TOE to restrict access to Customer data flowing through the TOE, or stored withn the TOE, respectively, based on Customer access authorizations.

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 Customer 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.

O.IDAUTH, OE.IDAUTH, and O.SECFUN support O.CMA by requiring that all administrators be uniquely identified and authenticated before they are granted access to TOE functions and data, and by ensuring that only authorized administrators are able to access TOE security functions.

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.

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.

©2012 Check Point Software Technologies Ltd. All Rights Reserved.

Classification: [Unrestricted]—For everyone

4.3.2. Security Objectives Upholding OSPs

Table 4-4 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 above. The table also maps the P.CUST 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 4-4 -Tracing of security objectives to OSPs

	[IDSSPP] OSPs							**ST**
	P.DETECT	**P.ANALYZ**	**P.MANAGE**	**P.ACCESS**	**P.ACCACT**	**P.INTGTY**	**P.PROTCT**	**P.CUST**
O.IDAUTH			✓	✓	✓			✓
O.SINUSE								
O.MEDIAT								✓
O.SECSTA								
O.ENCRYP								
O.SELPRO								
O.AUDREC[15]	✓				✓			
O.ACCOUN								
O.SECFUN			✓	✓				✓
O.LIMEXT								
O.PROTCT[16]			✓	✓				

[15] 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.

[16] 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.

©2012 Check Point Software Technologies Ltd. All Rights Reserved.

Classification: [Unrestricted]—For everyone

	[IDSSPP] OSPs							ST
	P.DETECT	**P.ANALYZ**	**P.MANAGE**	**P.ACCESS**	**P.ACCACT**	**P.INTGTY**	**P.PROTCT**	**P.CUST**
O.IDSENS	✓							
O.IDANLZ		✓						
O.RESPON								
O.OFLOWS							✓	
O.INTEGR						✓		
O.MAC								✓
O.CMA								✓
O.VPN								
O.FAULT								
NOE.INSTALL[17]			✓					
NOE.ADMTRA			✓					
NOE.PHYSICAL							✓	
NOE.CREDEN			✓					
OE.SINGEN								
OE.IDAUTH			✓	✓	✓			✓
OE.VPN								
OE.VLAN								✓

[17] 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.

©2012 Check Point Software Technologies Ltd. All Rights Reserved.

Classification: [Unrestricted]—For everyone

4.3.3. Security Objectives Upholding Assumptions

Table 4-5 maps security objectives for the operational environment to assumptions made in section 3.2. Each assumption traces to 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 seen that each security objective for the environment is traced to at least one environment consideration.

Table 4-5- 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			
NOE.INSTALL		[IDSSPP]	
NOE.ADMTRA			
NOE.PHYSICAL	[IDSSPP]	[IDSSPP]	
NOE.CREDEN		[IDSSPP]	
OE.SINGEN			[TFF-PP]
OE.IDAUTH			
OE.VPN			
OE.VLAN			

©2012 Check Point Software Technologies Ltd. All Rights Reserved.

Classification: [Unrestricted]—For everyone

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.

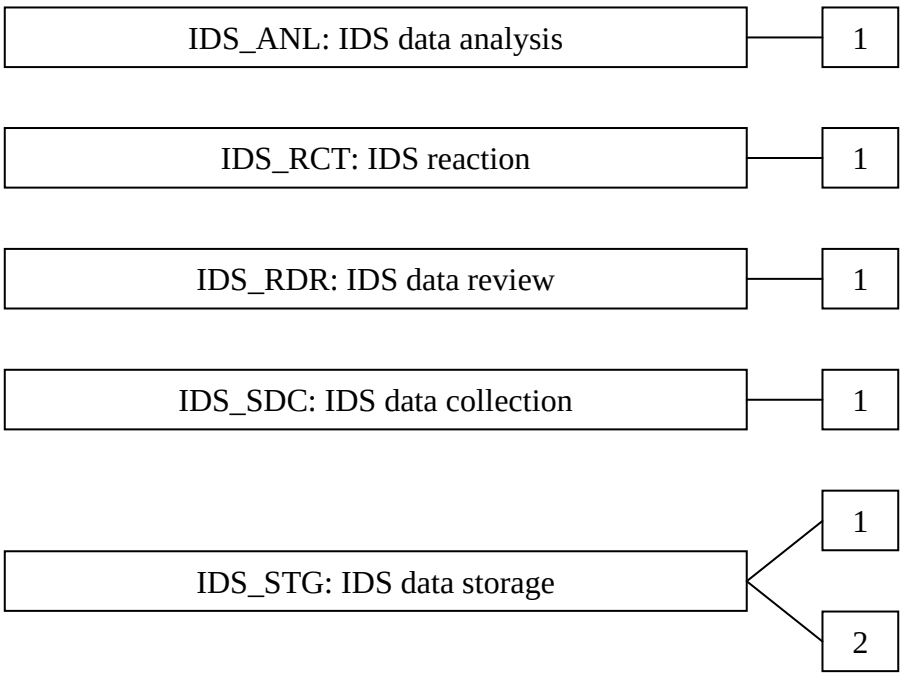
> "*A family of IDS requirements was created to specifically address the data collected and analyzed by an IDS. The audit family of the CC (FAU) was used as a model for creating these requirements. The purpose of this family of requirements is to address the unique nature of IDS data and provide for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



©2012 Check Point Software Technologies Ltd. All Rights Reserved.

Classification: [Unrestricted]—For everyone

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.

©2012 Check Point Software Technologies Ltd. All Rights Reserved.

Classification: [Unrestricted]—For everyone

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.

©2012 Check Point Software Technologies Ltd. All Rights Reserved.

Classification: [Unrestricted]—For everyone

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.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*].

©2012 Check Point Software Technologies Ltd. All Rights Reserved.

Classification: [Unrestricted]—For everyone

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

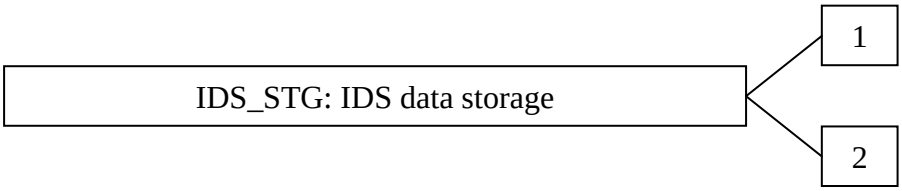
b) [assignment: *other additional information*].

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*].

©2012 Check Point Software Technologies Ltd. All Rights Reserved.

Classification: [Unrestricted]—For everyone

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.

©2012 Check Point Software Technologies Ltd. All Rights Reserved.

Classification: [Unrestricted]—For everyone

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 correspond to containers of network traffic information, including IPv4 packets, and network interfaces.

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.
D.TSF	TSF data is maintained by the TOE on three levels: MDS, per-CMA, and per-VS. There are five broad categories of TSF data objects: security policy (including network object and topology definitions), audit trails, user database, ICA database, and status monitoring data.

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). Subject security attributes are described for FIA_USB.1 /IFF. In addition, S.VS and S.CMA subjects are each statically associated with a Customer identifier security attribute that is used for restricting administrator authorizations.

S.VS	A Virtual System is an active entity within the INSPECT virtual machine environment that executes programs in its own separate execution domain on a VSX gateway, processing IPv4 packets (D.PACKET) and network information flows (D.INFO), reading and writing them from gateway interfaces.
S.CMA	A Customer Management Add-on is an active entity within the Provider-1 installation. Administrative users bind to this subject in order to perform management operations on TSF data (D.TSF).
S.MDS	The Multi-Domain Server subject maintains TSF data (D.TSF) for the Provider-1 installation as a whole. Administrative users bind to this subject in order to perform global and multi-CMA management operations.

©2012 Check Point Software Technologies Ltd. All Rights Reserved.

Classification: [Unrestricted]—For everyone

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 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 Virtual System (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.
U.VPNPEER	A peer VPN gateway is a special case of U.USER that establishes a trusted channel with the Virtual System (S.VS).
U.ADMIN	A human user that binds to the TOE in order to perform administrative operations. U.ADMIN may bind to a specific Customer subject (S.CMA) or to the MDS subject (S.MDS).
U.OPSEC	An authenticated external IT entity that binds to a CMA (S.CMA) over a SIC-protected trusted path, in order to perform restricted operations on TSF data using OPSEC client APIs (see section 1.5.3.12).

©2012 Check Point Software Technologies Ltd. All Rights Reserved.

Classification: [Unrestricted]—For everyone

6.1.4. Security Function Policies

6.1.4.1. Mandatory Access Control Policy

The TOE's virtualization security functionality is modeled using the Mandatory Access Control Policy. Information (D.INFO) can flow between Virtual Systems (S.VS) only through connections to virtual networking entities (Virtual Routers or Virtual Switches) explicitly defined by an authorized System administrator.

Information may also flow to Provider-1 subjects in the form of audit records and IDS System data. The SFP establishes a management hierarchy restricting the flow of such information from a Virtual System to CMAs associated with the same Customer.

This SFP ensures that a VSX gateway connected to multiple, independent and independently managed networks does not introduce any information flows between these networks except as explicitly configured by an authorized System administrator.

6.1.4.2. Traffic Filter SFP

The TOE's 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, U.RAUSER, and U.VPNPEER) bound to TOE Virtual Systems (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 that are received by the TOE over IPSec or SSL VPN tunnels established between the TOE and an authorized external IT entity. This traffic is considered to be authenticated by the nature of the VPN tunnel, which provides assured identification of its end points in accordance with FTP_ITC.1.

The authenticated VPN peer may be a remote access client that represents a human user (remote access VPN), or a VPN gateway that represents an entire VPN domain. In the latter case, authentication applies to the identity of the VPN peer gateway, rather than to the presumed identity of the external IT entity sending the information from the peer's VPN domain.

6.1.4.3. 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. TOE Virtual Systems (S.VS) apply decrypt-and-verify and encrypt-and-authenticate operations on incoming and outbound information, respectively, in accordance with the rules of this SFP.

©2012 Check Point Software Technologies Ltd. All Rights Reserved.

Classification: [Unrestricted]—For everyone

6.2. Security Functional Requirements

6.2.1. Summary of TOE Security Functional Requirements

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

The requirements were drawn from all claimed protection profiles; additional requirements have also been added to address the VPN objectives. The source for each requirement is denoted in column 3 of Table 6-1 as follows:

TFF Requirement drawn from [TFF-PP].

IDS Requirement drawn from [IDSSPP].

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

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

VIRT Requirement added to address virtualization objectives

VPN Requirement added to address VPN objectives[18]

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 [TFF-PP] as described in column 4 of Table 6-1 below, and in relation to [IDSSPP] 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**	
			TFF PP	**IDSS 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**

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

©2012 Check Point Software Technologies Ltd. All Rights Reserved.

Classification: [Unrestricted]—For everyone

Functional Component		Source PP(s)	CC Operations Applied	
			TFF PP	IDSS PP
FAU_SAR.3	**Selectable audit review**	**All**	**Refinement**	**Refinement**
FAU_SEL.1	**Selective audit**	**IDS**		**Assignment**
FAU_STG.2	**Guarantees of audit data availability**	**All**	**Hierar-chical, 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**	**TFF**	**None**	
FCS_COP.1 /3DES		**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 /TFF	**Subset information flow control**	**TFF**	**Refinement**	
FDP_IFC.1 /VPN		**VPN**	**Assignment**	
FDP_IFC.2	**Complete information flow control**	**VIRT**	**Assignment**	
FDP_IFF.1 /TFF	**Simple security attributes**	**TFF**	**Refinement, assignment**	
FDP_IFF.1 /VPN		**VPN**	**Assignment**	

©2012 Check Point Software Technologies Ltd. All Rights Reserved.

Classification: [Unrestricted]—For everyone

Functional Component		Source PP(s)	CC Operations Applied	
			TFF PP	IDSS PP
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	TFF	Hierar-chical	
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	Refine-ment, assignment	Assignment
FIA_UAU.1	Timing of authentication	All	Refinement	Assignment
FIA_UAU.4	Single-use authentication mechanisms	TFF	None	
FIA_UAU.5	Multiple authentication mechanisms	Other	Assignment	
FIA_UAU.7	Protected authentication feedback	Other	None	
FIA_UID.2	User identification before any action	All	None	Hierarchical
FIA_USB.1 /Admin	User-Subject Binding	Other	Refinement, assignment	
FIA_USB.1 /IFF		VIRT	Refinement, assignment	
FMT_MOF.1	Management of security functions behavior	All	Refine-ment, Assignment	Refinement, Assignment
FMT_MSA.1	Management of security attributes	VIRT	Assignment	
FMT_MSA.3 /IFF	Static attribute initialization	TFF	Refinement	
FMT_MSA.3 /MAC		VIRT	Assignment, selection	
FMT_MTD.1	Management of TSF data	IDS		Refinement, Assignment
FMT_REV.1 /Admin	Revocation	Other	Assignment, selection	

©2012 Check Point Software Technologies Ltd. All Rights Reserved.

Classification: [Unrestricted]—For everyone

Functional Component		Source PP(s)	CC Operations Applied	
			TFF PP	IDSS PP
FMT_REV.1 /User		**Other**	**Refinement, assignment, selection**	
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**
IDS_STG(EXP).1	**Guarantee of System Data Availability**	**IDS**		**Explicit, assignment, selection refinement**

©2012 Check Point Software Technologies Ltd. All Rights Reserved.

Classification: [Unrestricted]—For everyone

Functional Component		Source PP(s)	CC Operations Applied	
			TFF PP	IDSS PP
IDS_STG(EXP).2	**Prevention of System data loss**	**IDS**		**Explicit, refinement, selection**

SFRs are listed in the table above in alphabetical order to support using the table as a reference. The following subsections group these requirements according to their semantics, as follows:

The first subsection introduces requirements for TOE VLAN support and virtualization. VLAN tagging can support logical interfaces that are used by the TOE for user-subject binding. The TOE's virtualization requirements are then specified – users of the TOE are defined as domains or enclaves that bind to the TOE via physically or logically distinct interfaces, and issue information flow requests through the TOE. The TOE enforces independent rule sets for these users, and applies access control requirements to inter-domain data communications. A subsequent subsection details TOE authentication requirements for the various user categories.

The TOE's information flow control requirements are then specified: traffic filtering, VPN, and NAT. Cryptographic support and IDS/IPS requirements are identified in separate subsections.

Finally, TOE security management, audit, and self-protection capabilities are specified.

6.2.2. VLAN Support and Virtualization

6.2.2.1. 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.

©2012 Check Point Software Technologies Ltd. All Rights Reserved.

Classification: [Unrestricted]—For everyone

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

FDP_ITC.2.1 The TSF shall enforce the **Mandatory Access Control Policy** 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 Policy 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**.

©2012 Check Point Software Technologies Ltd. All Rights Reserved.

Classification: [Unrestricted]—For everyone

6.2.2.3. Complete information flow control (FDP_IFC.2)

FDP_IFC.2.1 The TSF shall enforce the **Mandatory Access Control Policy** on **information flowing through the TOE (D.INFO), subjects: Virtual Systems (S.VS) and CMAs (S.CMA),** 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), as well as Provider-1 subjects (S.CMA) which may receive controlled information in the form of audit records and IDS System data.*

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.

The Mandatory Access Control Policy also establishes a management hierarchy restricting the flow of information from a Virtual System to CMAs associated with the same Customer.

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

FDP_IFF.1.1 The TSF shall enforce the **Mandatory Access Control Policy** 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 CMA subjects (S.CMA):

- **Customer identifier;**

c) For information (D.INFO):

- **VSID**.

©2012 Check Point Software Technologies Ltd. All Rights Reserved.

Classification: [Unrestricted]—For everyone

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:

a) Information may flow between a Virtual System and a CMA or between two CMAs only if both subjects are associated with the same Customer identifier.

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

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

FDP_ETC.2.1 The TSF shall enforce the **Mandatory Access Control Policy** 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.*

©2012 Check Point Software Technologies Ltd. All Rights Reserved.

Classification: [Unrestricted]—For everyone

6.2.3. Identification and Authentication

6.2.3.1. 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) User identity;

b) Authentication data;

c) Authorisations; and

d) **Group memberships; and**

e) Assigned set of Customers.

6.2.3.2. 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.

6.2.3.3. Timing of authentication (FIA_UAU.1)

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

a) ARP;

b) ICMP;

c) Check Point RDP;

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

e) Unauthenticated information flows permitted by the 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:

The TOE also generates ARP responses on behalf of hosts for which Network Address Translation (NAT) is performed by the TOE.

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.

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.

©2012 Check Point Software Technologies Ltd. All Rights Reserved.

Classification: [Unrestricted]—For everyone

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 from workstations on which remote access VPN client software has not been previously installed. TOE support for SSL VPN is included in the TOE boundary; however, the downloadable SSL VPN client itself is considered to be outside the TOE.

6.2.3.4. Multiple authentication mechanisms (FIA_UAU.5)

FIA_UAU.5.1 The TSF shall provide **single-use authenticator and cryptographic protocol mechanisms, and shall provide support for passing user passwords to external authentication servers in the IT environment** 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) Human administrators (U.ADMIN) shall authenticate to the TOE using a TLS certificate-based authentication mechanism, or using single-use passwords authenticated with the support of the IT environment;

b) OPSEC clients (U.OPSEC) shall authenticate to the TOE using a TLS certificate-based authentication mechanism;

c) Human users and external IT entities sending authenticated traffic through the TOE, decrypted and verified in accordance with the VPN SFP, shall authenticate to the TOE using TLS or IKE or L2TP authentication mechanisms based on:

- **Certificates;**
- **Pre-shared secrets; or**
- **Single-use passwords authenticated with the support of the IT environment;**

d) Authorized external IT entities communicating with the TOE shall authenticate to the TOE using IKE or TLS authentication mechanisms or using single-use authenticator-based authentication mechanisms.

6.2.3.5. 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.

6.2.3.6. Protected authentication feedback (FIA_UAU.7)

FIA_UAU.7.1 The TSF shall provide only obscured feedback to the user while the authentication is in progress.

Application Note: Obscured feedback implies the TSF does not produce a visible display of any authentication data entered by a user, such as through a keyboard (e.g., echo the

©2012 Check Point Software Technologies Ltd. All Rights Reserved.

Classification: [Unrestricted]—For everyone

password on the terminal). It is acceptable that some indication of progress be returned instead, such as a period returned for each character sent.

6.2.3.7. 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 TRAFFIC FILTER and VPN SFPs;

c) The group membership or memberships used to enforce the TRAFFIC FILTER SFP;

d) The VSID used to enforce the Mandatory Access Control Policy.

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 identified by the VSID and presumed source network identifier attributes associated with the information. Both attributes are associated with auditable events and are used to enforce the TRAFFIC FILTER and VPN SFPs;

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 protocol. Any group memberships associated with the user identity can be used to enforce the TRAFFIC FILTER SFP, and the user identity is associated with auditable events.

d) The identity for users establishing a IPSec/L2TP tunnel is established from the user identity transferred as part of the L2TP protocol. In addition, the client computer identity transferred as part of the IKE protocol is also associated with auditable events;

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 Policy[19], then:

- **The VSID associated with the information assumes the VSID of the other Virtual System; and**

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

©2012 Check Point Software Technologies Ltd. All Rights Reserved.

Classification: [Unrestricted]—For everyone

- **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**.

6.2.3.8. 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) Association of a user with Customer assignments and administrator authorisations.

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 user identity for a human user associated with any administrator role or for an OPSEC client is associated with the subject acting on the user's behalf in the process of the establishment of the authenticated trusted path to the CMA (S.CMA) or MDS (S.MDS);

b) The user's Customer assignments and administrator authorisations for a human user binding to the MDS are associated with the subject (S.MDS);

c) A user may bind to a CMA subject (S.CMA) only if the user is associated with the CMA's defined Customer; the subject is then associated with this Customer attribute, as well as the user's authorisations for this Customer association.

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: **no additional rules**.

©2012 Check Point Software Technologies Ltd. All Rights Reserved.

Classification: [Unrestricted]—For everyone

6.2.4. Information Flow Control (Traffic Filtering and VPN)

6.2.4.1. 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 Virtual System subject (S.VS), which performs operations on information (D.INFO) in the form of IPv4 packets (D.PACKET) on its behalf.*

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

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

a) subjects: TOE Virtual Systems (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.

©2012 Check Point Software Technologies Ltd. All Rights Reserved.

Classification: [Unrestricted]—For everyone

6.2.4.3. 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;
- **group memberships of remote access VPN user, if established in accordance with FDP_IFF.1 /VPN and FIA_USB.1 /IFF;**

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 **System** 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;

©2012 Check Point Software Technologies Ltd. All Rights Reserved.

Classification: [Unrestricted]—For everyone

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 System administrator.

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

a) Wire Mode: an authorized System 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.

©2012 Check Point Software Technologies Ltd. All Rights Reserved.

Classification: [Unrestricted]—For everyone

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.

6.2.4.4. 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 (S.VS) security attributes:

- **VSID;**
- **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 in-

©2012 Check Point Software Technologies Ltd. All Rights Reserved.

Classification: [Unrestricted]—For everyone

formation before enforcing the TRAFFIC FILTER 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 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 Virtual System (by VSID); 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 Virtual System (by VSID), 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 System 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 Virtual System; and**
- **the destination address in the information is defined in the VPN domain of the subject Virtual System;**

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;

©2012 Check Point Software Technologies Ltd. All Rights Reserved.

Classification: [Unrestricted]—For everyone

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**.

6.2.4.5. 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.

Application Note: *FDP_RIP is a requirement derived from [TFF-PP]. The 'objects' defined in [TFF-PP] 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.

6.2.4.6. 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[20] or another 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**.

6.2.4.7. 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.

6.2.4.8. 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.

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

©2012 Check Point Software Technologies Ltd. All Rights Reserved.

Classification: [Unrestricted]—For everyone

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

6.2.5. Cryptographic support (FCS)

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

FCS_CKM.1.1 The TSF shall generate **RSA** 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** that meet the following: **NIST SP 800-90 and FIPS PUB 140-2 (level 1)**.

6.2.5.2. 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 PUB 140-2 (level 1)**.

6.2.5.3. 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 **IKE** that meets the following: **RFC 2409, with the following instantiation:**

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

b) The Diffie-Hellman key exchange[21] 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), and group 24 in accordance with RFC 5114 (2048-bit MODP with 256-bit Prime Order Subgroup);

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

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

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

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

[21] 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).

©2012 Check Point Software Technologies Ltd. All Rights Reserved.

Classification: [Unrestricted]—For everyone

- **Authentication with digital signatures: The TSF shall use RSA;**
- **The TSF shall be capable of checking the validity of the X.509v3 certificate path, and at option of the authorized System administrator, check for certificate revocation using the HTTP (RFC2616), LDAP (RFC1777), or OCSP (RFC2560) protocols;**
- **Authentication with a pre-shared key: The TSF shall allow authentication using a pre-shared key; and**
- **The TSF shall support a Hybrid Mode[22] 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**.

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

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

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

b) The TSF shall be capable of authenticating SIC and SSL VPN sessions using the following methods as configured by the security administrator:

- **Authentication with digital signatures: The TSF shall use RSA;**
- **For SSL VPN session establishment, the TSF shall be capable of checking the validity of the X.509v3 certificate path, and at option of the authorized System administrator, check for certificate revocation using the HTTP (RFC2616), LDAP (RFC1777), or OCSP (RFC2560) protocols;**
- **For SIC session establishment, the TSF shall check for certificate revocation using internally-distributed X.509v3 certificates;**
- **The TSF shall support single-use password-based user authentication, 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**.

6.2.5.5. 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: **no standard**.

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

©2012 Check Point Software Technologies Ltd. All Rights Reserved.

Classification: [Unrestricted]—For everyone

6.2.5.6. *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).

6.2.5.7. *Cryptographic operation (FCS_COP.1 /3DES)*

FCS_COP.1.1 The TSF shall perform **encryption and decryption of SSL VPN traffic** in accordance with a specified cryptographic algorithm: **Triple Data Encryption Standard (DES)** and cryptographic key sizes **that are 192 binary digits in length** that meet the following: **FIPS PUB 46-3, NIST SP 800-67, and FIPS PUB 140-2 (Level 1)**.

6.2.5.8. *Cryptographic operation (FCS_COP.1 /ESP)*

FCS_COP.1.1 The TSF shall perform **encryption and decryption of IPSec VPN traffic** in accordance with specified cryptographic algorithms: **Triple Data Encryption Standard (DES); or Advanced Encryption Standard (AES)** and cryptographic key sizes **that are 192 binary digits in length for Triple DES; or 128 or 256 binary digits in length for AES** that meet the following: (**FIPS PUB 197 in CBC mode for AES; or NIST SP 800-67 and FIPS PUB 46-3 with Keying Option 1 (K1, K2, K3 are independent keys) for Triple DES, RFC 2406 (Encapsulating Security Payload (ESP)) and FIPS PUB 140-2 (Level 1)**.

6.2.5.9. *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** and cryptographic key sizes **that are 160 binary digits in length** that meet the following: **RFC 2104, FIPS PUB 198, RFC 2404 (The Use of HMAC-SHA-1-96 within ESP and AH) and FIPS PUB 140-2 (Level 1)**.

6.2.5.10. *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 and SHA-256** and cryptographic key sizes **not applicable** that meet the following: **FIPS PUB 180-2 and FIPS PUB 140-2 (Level 1)**.

6.2.5.11. *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** and cryptographic key sizes **1024, 2048 or 4096 binary digits in length** that meet the following: **PKCS #1 and FIPS PUB 140-2 (Level 1)**.

©2012 Check Point Software Technologies Ltd. All Rights Reserved.

Classification: [Unrestricted]—For everyone

6.2.5.12. 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 or 8192 binary digits in length (for Diffie Hellman groups 1, 2, 5, 14 and 24, 15, 16, 17 and 18, respectively)** that meet the following: **RFC 2631, RFC 3526, RFC 5114, and FIPS PUB 140-2 (Level 1)**.

6.2.6. Security Audit (FAU)

6.2.6.1. 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 basic level of audit; and

c) **The events listed in column "Auditable Event" of** 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, and the outcome (success or failure) of the event; and

b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, the additional information specified in **column three** of Table 6-2 Auditable Events.

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.		All
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		Other

©2012 Check Point Software Technologies Ltd. All Rights Reserved.

Classification: [Unrestricted]—For everyone

Functional Component	Auditable Event	Additional Audit Record Contents	Source PPs
	of a threshold.		
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
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; any applicable cryptographic mode(s) of operation, subject attributes and object attributes.	TFF
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.	TFF
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.	Other
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

©2012 Check Point Software Technologies Ltd. All Rights Reserved.

Classification: [Unrestricted]—For everyone

Functional Component	Auditable Event	Additional Audit Record Contents	Source PPs
FMT_MOF.1	Use of the functions listed in this requirement pertaining to audit.	The identity of the authorized administrator performing the operation.	TFF
	All modifications in the behavior of the functions of the TSF.		IDS
FMT_MSA.1	All modifications of the values of security attributes.		VIRT
FMT_MSA.3	Modifications of the default setting of permissive or restrictive rules. All modifications of the initial value of security attributes.		VIRT
FMT_MTD.1	All modifications to the values of TSF data.	The new value of the TSF data.	Other
FMT_REV.1	All attempts to revoke user security attributes.		Other
	All modifications to the values of security attributes associated with objects controlled by the Mandatory Access Control Policy.		Other
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
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

©2012 Check Point Software Technologies Ltd. All Rights Reserved.

Classification: [Unrestricted]—For everyone

Functional Component	Auditable Event	Additional Audit Record Contents	Source PPs
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

6.2.6.2. 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.

6.2.6.3. Audit review (FAU_SAR.1)

FAU_SAR.1.1 The TSF shall provide **authorized roles defined in FMT_SMR.1** with the capability to read **all audit trail data, constrained by the user's authorisations and Customer assignments,** 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.

6.2.6.4. 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.

6.2.6.5. 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;

©2012 Check Point Software Technologies Ltd. All Rights Reserved.

Classification: [Unrestricted]—For everyone

e) ranges of addresses;

f) type of event; and

g) success or failure of related event.

6.2.6.6. 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**.

6.2.6.7. 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.

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

FAU_STG.3.1 The TSF shall generate an alarm to the authorized **System** administrator if the audit trail exceeds **a limit defined by the authorized System administrator such that the amount of free disk space falls below an administrator-defined threshold**.

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

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

6.2.7. Security Management (FMT)

6.2.7.1. 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, constrained by the administrator's authorisations and Customer assignments**.

[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, as required in the application note for [CAPP] section 5.1.7.2.

©2012 Check Point Software Technologies Ltd. All Rights Reserved.

Classification: [Unrestricted]—For everyone

6.2.7.2. Management of security attributes (FMT_MSA.1)

FMT_MSA.1.1 The TSF shall enforce the **Mandatory Access Control Policy** to restrict the ability to query or modify the security attributes **Virtual System interface and Customer associations** to **an authorized System administrator, constrained by the administrator's authorisations and Customer assignments**.

6.2.7.3. Static attribute initialization (FMT_MSA.3 /MAC)

FMT_MSA.3.1 The TSF shall enforce the **Mandatory Access Control Policy** to provide restrictive default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2 The TSF shall allow the **authorized System administrator, constrained by the administrator's authorisations and Customer assignments** to specify alternative initial values to override the default values when an object or information is created.

6.2.7.4. Static attribute initialization (FMT_MSA.3 /IFF)

FMT_MSA.3.1 The TSF shall enforce the **TRAFFIC FILTER 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: *From [TFF-PP]:*

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.

6.2.7.5. 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, constrained by the administrator's authorisations and Customer assignments**.

6.2.7.6. Revocation of User Attributes (FMT_REV.1 /Admin)

FMT_REV.1.1 The TSF shall restrict the ability to revoke **administrator security attributes** associated with the users under the control of the TSF to **authorized administrators**.

FMT_REV.1.2 The TSF shall enforce the rules:

a) **Revocation of administrator security attributes shall be applicable to the administrator's next login. Existing administrator sessions may be terminated immediately by an authorized administrator**.

©2012 Check Point Software Technologies Ltd. All Rights Reserved.

Classification: [Unrestricted]—For everyone

6.2.7.7. Revocation of Object Attributes (FMT_REV.1 /User)

FMT_REV.1.1 The TSF shall restrict the ability to revoke **user security attributes** associated with **non-administrator** users under the control of the TSF to **authorized System administrators, constrained by the administrator's authorisations and Customer assignments**.

FMT_REV.1.2 The TSF shall enforce the rules:

a) **Revocation shall apply immediately after the security policy is installed by an authorized System administrator**.

6.2.7.8. Specification of management functions (FMT_SMF.1)

FMT_SMF.1.1 The TSF shall be capable of performing the following 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
	create, delete, modify, and view default information flow security policy rules that permit or deny information flows globally for all Customers	authorized administrator	TFF
	create, delete, modify, and view information flow security policy rules that permit or deny information flows for Virtual Systems for a specific Customer	authorized System administrator	TFF
	create, delete, modify, and view user attribute values defined in FIA_ATD.1 for administrator roles	authorized administrator	TFF
	create, delete, modify, and view user attribute values defined in FIA_ATD.1 for non-administrators	authorized System administrator	TFF
	enable and disable single-use authentication mechanisms in FIA_UAU.4	authorized administrator, authorized System administrator	TFF
	control of communication with authorized external IT entities	authorized System administrator	TFF

©2012 Check Point Software Technologies Ltd. All Rights Reserved.

Classification: [Unrestricted]—For everyone

Component	Management Function	Authorized Roles	Source PPs
	modify and set the time and date	no administrator role	TFF
	archive, create, delete, and empty the audit trail	authorized System administrator	TFF
	review the audit trail	authorized System administrator, OPSEC client	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 System administrator	TFF
	recover to the state following the last backup	authorized System administrator	TFF
	enable and disable remote administration from internal and external networks	authorized System administrator	TFF
	restrict addresses from which remote administration can be performed	authorized administrator, authorized System administrator	TFF
	modify the behaviour of the functions of System data collection, analysis and reaction	authorized System administrator	IDS
	enabling SIC trust between Provider-1 and a VSX gateway	authorized System administrator	Other
FMT_MSA.1	query, modify Virtual System interface and Customer associations	authorized System administrator	VIRT

©2012 Check Point Software Technologies Ltd. All Rights Reserved.

Classification: [Unrestricted]—For everyone

Component	Management Function	Authorized Roles	Source PPs
FMT_MSA.3 /MAC	specification of alternative initial values to override the default values for Virtual System interface and Customer associations	authorized System administrator	VIRT
FMT_MSA.3 /IFF	specification of default information flow security rules	authorized administrator	TFF
FMT_MTD.1	query IDS System and audit data	authorized System administrator, OPSEC client	IDS
	add IDS System and audit data	OPSEC client	IDS
	query and modify all other TOE data (other than IDS System and audit data)	Authorized administrator, authorized System administrator	IDS
	management of the thresholds and actions taken in case of imminent audit storage failure	authorized System administrator	Other

6.2.7.9. Security roles (FMT_SMR.1)

FMT_SMR.1.1 The TSF shall maintain the following roles: authorized administrator, authorized System administrator, **and OPSEC client**.

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

6.2.8. Protection of the TSF

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

FPT_ITT.1.1 The TSF shall protect TSF data from disclosure and modification when it is transmitted between separate parts of the TOE.

6.2.8.2. Reliable time stamps (FPT_STM.1)

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

©2012 Check Point Software Technologies Ltd. All Rights Reserved.

Classification: [Unrestricted]—For everyone

6.2.9. Fault Tolerance

6.2.9.1. 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**.

6.2.9.2. 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**.

6.2.9.3. 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.

6.2.9.4. 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**.

©2012 Check Point Software Technologies Ltd. All Rights Reserved.

Classification: [Unrestricted]—For everyone

6.2.10. Trusted path/channels (FTP)

6.2.10.1. Trusted Path (FTP_TRP.1)

FTP_TRP.1.1 The TSF shall provide a communication path between itself and local and remote users that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from modification or disclosure.

FTP_TRP.1.2 The TSF shall permit 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 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.

©2012 Check Point Software Technologies Ltd. All Rights Reserved.

Classification: [Unrestricted]—For everyone

6.2.11. IDS/IPS

6.2.11.1. 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) **stateful pattern matching of collected System data against INSPECT code fragments that represent potential violations of the enforcement of the SFRs**.

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) **Virtual System**.

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

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

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

IDS_RDR(EXP).1.1 The System shall provide **authorized System administrators and OPSEC clients** with the capability to read **all data, constrained by the user's authorisations and Customer assignments,** 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.

6.2.11.4. 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.

©2012 Check Point Software Technologies Ltd. All Rights Reserved.

Classification: [Unrestricted]—For everyone

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**

6.2.11.5. 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.

6.2.11.6. 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.

©2012 Check Point Software Technologies Ltd. All Rights Reserved.

Classification: [Unrestricted]—For everyone

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 any assurance component.

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

©2012 Check Point Software Technologies Ltd. All Rights Reserved.

Classification: [Unrestricted]—For everyone

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

©2012 Check Point Software Technologies Ltd. All Rights Reserved.

Classification: [Unrestricted]—For everyone

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
× Omitted IDS System PP mapping ✓ Mapping added in this ST

(Note: where a mapping exists in more than one PP, the corresponding mapping symbol is taken from either the firewall or IDS PP, in order of precedence.)

	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		✓				✓												✓	

©2012 Check Point Software Technologies Ltd. All Rights Reserved.

Classification: [Unrestricted]—For everyone

	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 /3DES						✓												✓	
FCS_COP.1 /ESP																		✓	
FCS_COP.1 /MAC		✓																✓	
FCS_COP.1 /Hash		✓				✓												✓	
FCS_COP.1 /Signature		✓				✓												✓	
FCS_COP.1 /DH		✓																✓	
FCS_CKM.4		✓				✓												✓	
FDP_ETC.2																	✓		
FDP_IFC.1 /TFF			☑																
FDP_IFC.1 /VPN																		✓	
FDP_IFC.2																	✓		
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_UAU.7	✓																		
FIA_UID.2	☑							☑	?										
FIA_USB.1 /Admin	✓						✓	✓											
FIA_USB.1 /IFF	✓						✓	✓									✓		
FMT_MOF.1	✘			☑					☑	☑	?								

©2012 Check Point Software Technologies Ltd. All Rights Reserved.

Classification: [Unrestricted]—For everyone

	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
FMT_MSA.1																	✓		
FMT_MSA.3 /MAC																	✓		
FMT_MSA.3 /IFF			☑	☑					☑										
FMT_MTD.1	×								?		?					?			
FMT_REV.1 /Admin									✓										
FMT_REV.1 /User																			
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	×						×		×		×					×			

©2012 Check Point Software Technologies Ltd. All Rights Reserved.

Classification: [Unrestricted]—For everyone

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.*

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, for administrators and for users sending information through the TOE, respectively. 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.

FIA_UAU.7 requires that authentication data is protected if feedback is provided during authentication.

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.1 ensures that users are authenticated at the TOE. FIA_UAU.4 was chosen in [TFF-PP] to ensure that some one-time authentication mechanism is used in all attempts to authenticate at the TOE from an internal or external network.

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 and/or a single-use password. FCS_CKM.2 /TLS defines the authentication and key distribution protocol to be used for SIC, and FCS_CKM.2 /IKE describes the requirement for IKE authentication.

©2012 Check Point Software Technologies Ltd. All Rights Reserved.

Classification: [Unrestricted]—For everyone

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 /TFF identifies the entities involved in the TRAFFIC FILTER information flow control SFP (i.e., users sending information to other users and vice versa). FDP_IFF.1 /TFF covers any traffic flowing through the TOE. It identifies the information security attributes that are used for information flow control, and the information flow control policies to be applied to each information flow.

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 /IFF ensures that there is a default deny policy for the information flow control security rules.

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 /IFF 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.

This component 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

©2012 Check Point Software Technologies Ltd. All Rights Reserved.

Classification: [Unrestricted]—For everyone

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 System 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.

FPT_ITT.1 was introduced to protect communication between distributed parts of the TOE (i.e. Provider-1 to appliance management traffic). FTP_TRP.1 provides the administrator with a trusted path between the management GUI and Provider-1. FCS_CKM.2 /TLS, FCS_COP.1 /3DES 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.

©2012 Check Point Software Technologies Ltd. All Rights Reserved.

Classification: [Unrestricted]—For everyone

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.2 requires the TSF to provide the capability to audit the actions of an individual user. FIA_USB.1 /Admin and FIA_USB.1 /IFF determine the binding of the user's identity used for auditing with the subject acting on his behalf, for administrators and for users sending information through the TOE, respectively.

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.2 requires that the audit trail must be complete. FAU_STG.3 and FAU_STG.4 ensure 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 determine the rules for associating the user identity which is associated with auditable events with a subject acting on behalf of the user, for administrators and for users sending information through the TOE, respectively.

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_MTD.1 restrict the use of these management functions to authorized administrator roles, as specified in Table 6-3.

©2012 Check Point Software Technologies Ltd. All Rights Reserved.

Classification: [Unrestricted]—For everyone

FMT_MSA.3 /IFF require 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.3 and FAU_STG.4 ensure 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).1 requires equivalent functionality for IDS System data.

FMT_REV.1 /Admin and FMT_REV.1 /User provide security attribute revocation capabilities for user security attributes, for administrator and non-administrator users, respectively.

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.

©2012 Check Point Software Technologies Ltd. All Rights Reserved.

Classification: [Unrestricted]—For everyone

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

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 System data.

©2012 Check Point Software Technologies Ltd. All Rights Reserved.

Classification: [Unrestricted]—For everyone

O.MAC *The TSF must control access to resources based on identity of subjects. The TSF must allow authorized users to specify which resources may be accessed by which subjects***.**

FDP_IFC.2 and FDP_IFF.1 /VS define the Mandatory Access Control Policy including the security attributes of subject (Virtual Systems) and objects (interfaces) used to enforce the policy.

FIA_USB.1 /IFF determines the binding of user identity, group memberships, and authorizations with the subject, in support of the enforcement of the MAC policy. FIA_ATD.1 supports this requirement by maintaining user identity and authorizations for individual users. 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 /MAC ensures that protection of named objects must be continuous, starting from object creation.

FMT_MSA.1 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.

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 TLSv1.0 cryptographic key distribution for SSL VPNs;
- FCS_COP.1 /3DES requires support for Triple DES for encryption and decryption of SSL VPN traffic;

©2012 Check Point Software Technologies Ltd. All Rights Reserved.

Classification: [Unrestricted]—For everyone

FCS_COP.1 /MAC, FCS_COP.1 /Hash, FCS_COP.1 /Signature and FCS_COP.1 /DH define requirements for HMAC-SHA-1, SHA-1 and SHA-256, RSA and Diffie Hellman, 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.

EAL 4 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.

©2012 Check Point Software Technologies Ltd. All Rights Reserved.

Classification: [Unrestricted]—For everyone

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	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	FMT_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_CKM.4	
FCS_CKM.1 /Sym		FCS_COP.1 /Admin**,** FCS_COP.1 /3DES **,** FCS_COP.1 /ESP, FCS_CKM.4	
FCS_CKM.2 /IKE	[FDP_ITC.1or FDP_ITC.2 or FCS_CKM.1],	FCS_CKM.1 /Asym, FCS_CKM.1 /Sym, FCS_CKM.4	
FCS_CKM.2 /TLS			

©2012 Check Point Software Technologies Ltd. All Rights Reserved.

Classification: [Unrestricted]—For everyone

SFR	CC dependency	ST dependency	Rationale
	FCS_CKM.4		
FCS_CKM.4	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1]	FCS_CKM.1 /Asym, FCS_CKM.1 /Sym	
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 /3DES			
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 /TFF	FDP_IFF.1	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 /TFF	FDP_IFC.1, FMT_MSA.3	FDP_IFC.1 /TFF, FMT_MSA.3 /IFF	
FDP_IFF.1 /VPN		FDP_IFC.1 /VPN, FMT_MSA.3 /IFF	
FDP_IFF.1 /VS		FDP_IFC.2, FMT_MSA.3 /MAC	
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 (VLAN tags). These are exchanged with the physically-connected bridge device, protected outside of the TOE in accordance with

©2012 Check Point Software Technologies Ltd. All Rights Reserved.

Classification: [Unrestricted]—For everyone

SFR	CC dependency	ST dependency	Rationale
			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	**FID_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_UAU.7	FIA_UAU.1	FIA_UAU.1	
FIA_UID.2	None		
FIA_USB.1 /Admin	FIA_ATD.1	FIA_ATD.1	
FIA_USB.1 /IFF			
FMT_MOF.1	FMT_SMF.1, FMT_SMR.1	FMT_SMF.1, FMT_SMR.1	
FMT_MSA.1	[FDP_ACC.1 or FDP_IFC.1], FMT_SMF.1, FMT_SMR.1	FDP_IFC.1/TFF, FMT_SMF.1, FMT_SMR.1	
FMT_MSA.3 /MAC	FMT_MSA.1, FMT_SMR.1	FMT_MSA.1, FMT_SMR.1	
FMT_MSA.3 /IFF		FMT_MOF.1, FMT_SMR.1	Justification for satisfying the dependency using FMT_MOF.1 instead of FMT_MSA.1 is as given in [TFF-PP].
FMT_MTD.1	FMT_SMF.1, FMT_SMR.1	FMT_SMF.1, FMT_SMR.1	
FMT_REV.1 /Admin	FMT_SMR.1	FMT_SMR.1	
FMT_REV.1 /User			
FMT_SMF.1	None		

©2012 Check Point Software Technologies Ltd. All Rights Reserved.

Classification: [Unrestricted]—For everyone

SFR	CC dependency	ST dependency	Rationale
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	FPT_STM.1	FPT_STM.1	
IDS_ANL(EXP).1	IDS_SDC.1	IDS_SDC(EXP).1	
IDS_RCT(EXP).1	IDS_ANL.1	IDS_ANL(EXP).1	
IDS_RDR(EXP).1	IDS_SDC.1	IDS_SDC(EXP).1	
IDS_STG(EXP).1	IDS_SDC.1	IDS_SDC(EXP).1	
IDS_STG(EXP).2	IDS_STG.1	IDS_STG(EXP).1	
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		

©2012 Check Point Software Technologies Ltd. All Rights Reserved.

Classification: [Unrestricted]—For everyone

SFR	CC dependency	ST dependency	Rationale
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.4, ADV_TDS.3, ADV_IMP.1, AGD_OPE.1, AGD_PRE.1, ATE_DPT.1	ADV_ARC.1, ADV_FSP.4, ADV_TDS.3, ADV_IMP.1, AGD_OPE.1, AGD_PRE.1, ATE_DPT.1	Consistent with EAL4

©2012 Check Point Software Technologies Ltd. All Rights Reserved.

Classification: [Unrestricted]—For everyone

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 6.2.5 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 6.2.5 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 VSX 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)	FCS_CKM.2 /IKE	Vendor assertion
RFC 2406 (ESP)	FCS_COP.1 /ESP	
FIPS 140-2 Level 1	FCS_CKM.1 FCS_COP.1 (all iterations)	Vendor assertion[24]
Hash_DRBG (SHA-256) as per NIST SP 800-90	FCS_CKM.1 /Asym, FCS_CKM.1 /Sym FCS_CKM.2 /IKE	Vendor assertion
Triple DES in CBC modes as per FIPS PUB 46-3	FCS_COP.1 /3DES , FCS_COP.1 /ESP	Cert. #824 and #825
AES in CBC mode as per FIPS PUB 197	FCS_COP.1 /Admin, FCS_COP.1 /ESP	Cert. #1130
HMAC-SHA-1 as per RFC 2104, FIPS PUB 198 and RFC 2404	FCS_COP.1 /MAC	Cert. #642 and #643
SHA-1 as per NIST PUB FIPS 180-2	FCS_COP.1 /Hash	Cert. #1053 and #1054
SHA-256 as per NIST PUB FIPS 180-3	FCS_COP.1 /Hash	Vendor assertion

[24] A previous version of the product's cryptographic library was validated to FIPS 140-2 level 1 (see Cert.#722). The vendor intends to perform a FIPS 140-2 level 1 or higher validation in parallel to the evaluation of the TOE, and will replace the vendor assertion with a FIPS 140 certificate number when such is available.

©2012 Check Point Software Technologies Ltd. All Rights Reserved.

Classification: [Unrestricted]—For everyone

RSA digital signatures as per PKCS#1	FCS_COP.1 /Signature	Cert. #66 and #537
TLSv1.0 as per RFC 2246	FCS_CKM.2 /TLS	Vendor assertion
Diffie-Hellman as per RFC 2631, RFC 3526, and RFC 5114	FCS_COP.1 /DH	Vendor assertion

©2012 Check Point Software Technologies Ltd. All Rights Reserved.

Classification: [Unrestricted]—For everyone

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 VSX gateways and Provider-1 management components.

Check Point VSX gateways can be configured to selectively generate audit records for matched security policy rules, including both traffic filtering (packet inspection) events and VPN key exchange and encrypted packet handling events. Each Virtual System on the gateway maintains its own log record queue.

Audit records are forwarded online to Provider-1 (in batches of every two seconds or 50 log records) for storage and for audit review. Each Virtual System forwards log records to its defined Provider-1 CMA log servers; the log server must belong to the same Customer as the Virtual System. Each CMA maintains a separate log database on the Provider-1 installation. In a management high-availability configuration, the gateway can forward its log records to both active and standby CMAs. Backup log servers can also be configured in case connectivity is lost to the CMAs.

In a VSX cluster configuration, Virtual Systems on each gateway forward their log records to Provider-1 CMAs independently; multiple records referring to a single connection are consolidated by the CMA.

Each CMA also maintains a separate log file database for audit records related to administrator access and management operations. The MDS itself also maintains its own audit log database for recording events related to the authorized administrators and the MDS.

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- TSS Mapping for 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 VSX gateway or Provider-1 host boots up, and cannot be disabled by an administrator.

Audit records are generated on start-up for both VSX gateway and Provider-1 host.</td></tr>
</table>
</td></tr>
</table>

©2012 Check Point Software Technologies Ltd. All Rights Reserved.

Classification: [Unrestricted]—For everyone

Component	Description of mechanism		
			Gateway shut-down can be identified by cluster state transition logs and by log records generated by the CMA when connectivity to the gateway is lost. Authorized administrator-initiated CMA start-up and shutdown are audited events.
	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	Logging of authorized System administrator logins to the SmartView Tracker management GUI.
	FAU_SAR.2	Unsuccessful attempts to read information from the audit records	Logging of authorized System administrator login failures to the SmartView Tracker management GUI.
	FAU_SEL.1	All modifications to the audit configuration that occur while the audit collections functions are operating	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 and VPN key generation, VPN key exchanges.
	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

©2012 Check Point Software Technologies Ltd. All Rights Reserved.

Classification: [Unrestricted]—For everyone

Component	Description of mechanism		
	FIA_UAU.5	The final decision on authentication.	establishment, and user authentication events. All log records include both presumed source address and user identity (for successful authentication events).
	FIA_UID.2	All use of the user identification mechanism.	Administrator login events are logged, 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 start-up and shutdown of CMAs and MDSs, user account and certificate management, audit trail log-switches and purges.
	FMT_MSA.1	All modifications of the values of security attributes.	Modifications to the MDS database including interface associations with Virtual Systems are logged by the MDS.
	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	Logging of security policy modifications,

©2012 Check Point Software Technologies Ltd. All Rights Reserved.

Classification: [Unrestricted]—For everyone

Component	Description of mechanism		
		of TSF data	user management.
	FMT_REV.1	All attempts to revoke user security attributes.	All user database update operations are audited.
		All modifications to the values of security attributes associated with objects controlled by the Mandatory Access Control Policy.	Modifications to the MDS database including interface associations with Virtual Systems are logged by the MDS.
	FMT_SMF.1	Use of the management functions.	Administrator logins to the management GUIs are logged, as well as all Provider-1 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.
	FPT_FLS.1	Failure of the TSF	Provider-1 generates a log record when a VSX 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 CMA.
	FPT_TST.1	Execution of the TSF self tests and the results of the tests.	The Management GUIs display VSX gateway and Provider-1 host operational status, as well as policy installation status. Log records and alerts can be generated whenever a failure is detected.
	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 System administrator can selectively configure logging for each IDS/IPS event.

©2012 Check Point Software Technologies Ltd. All Rights Reserved.

Classification: [Unrestricted]—For everyone

Component	Description of mechanism
	IDS_RDR.1 | Reading of information from the System data. Unsuccessful attempts to read information from the System data. | Logging of authorized System 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, as well as the relevant Virtual System identification. 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 System administrators use the SmartView Tracker 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. Authorized administrators may also use SmartView Tracker to review MDS-level audit trails. OPSEC clients access audit records via non-TOE applications using the LEA OPSEC API (see section 1.5.3.12). LEA is a well-defined API that provides log record information, including a data dictionary that assists the application in interpreting the information. In each case, the management GUI or OPSEC API provides access only to audit records that are maintained by the CMA or MDS to which the client has connected. Customer assignments and Audit Logs authorisations for the administrator are verified before providing access to audit data.
FAU_SAR.2	The Provider-1 installation is protected from any external access by a VSX 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. Provider-1 determines the authorisations of the identified user; only users defined in the relevant CMA or MDS as having log review privileges can view the contents of the audit log database.
FAU_SAR.3	SmartView Tracker allows the authorized System 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 VSX 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

©2012 Check Point Software Technologies Ltd. All Rights Reserved.

Classification: [Unrestricted]—For everyone

Component	Description of mechanism
	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 Virtual System by the authorized System administrator determines which Packet Inspection and VPN events generate audit records, based on event type. The policy can also be configured to inhibit log generation for an identified Virtual System, set of presumed source addresses, or VPN-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 MDS and CMA log databases on the Provider-1 installation, protected from any external access by a VSX 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. Provider-1 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 Provider-1 events, respectively. There is no interface allowing modification of audit records. The LEA API provides only read-only access to audit records. VSX 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 Provider-1 host falls below a predefined CMA threshold, the CMA stops collecting audit records. As explained above, VSX gateways will queue the records, and eventually start logging them to the local disk, until connectivity is resumed (i.e. until an authorized System administrator frees up storage on the Provider-1 host or redirects the gateway to log to another log server). If the disk space on the VSX 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 VSX gateways and Provider-1 hosts.
7.1.2. Cryptographic support (FCS)	
FCS_CKM.1 /Asym	RSA keys are generated by the TOE in support of both VPN and SIC functionality. The TOE supports key generation with key lengths of 1024, 2048 and 4096 bits. RSA key generation uses the underlying FIPS 140-2 compliant SP 800-90 DRBG described

©2012 Check Point Software Technologies Ltd. All Rights Reserved.

Classification: [Unrestricted]—For everyone

Component	Description of mechanism
	below for FCS_CKM.1 /Sym. SIC keys are generated by the ICA, described in section 1.5.3.11 (see also below for FCS_CKM.2 /TLS). VSX 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. Virtual System VPN keys are generated by the CMA. 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 CMA to the VSX gateway. Note: The ICA can also generate VPN certificates internally, without relying on an external certificate authority in the IT environment. However, the evaluated configuration does not allow external access to the Security Management server, thereby preventing access to ICA CRLs.
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 PRNG into an entropy pool from various sources, including 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 PRNG.
FCS_CKM.2 /IKE, FCS_COP.1 /ESP, FCS_COP.1 /MAC, FCS_COP.1 /Hash, FCS_COP.1 /Signature, FCS_COP.1 /DH	Each Virtual System on a VSX gateway includes a separate VPN daemon that maintains a set of active Security Associations for IKE, IPSec, and SSL VPN (TLS) 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. IKE phase 1 is supported using either Main Mode (default) or Aggressive Mode, in accordance with [RFC2409]. The TOE supports Diffie-Hellman groups 1, 2, 5, 14 through 18, and 24. SHA-1 is used as the pseudo random function. Gateway authentication can be configured to use either RSA 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 VSX gateway performs X.509v3 certificate path validation, and as configured by an administrator, checks for certificate revocation using the HTTP ([RFC2616]), LDAP ([RFC1777]), or OCSP ([RFC2560]) protocols. The TOE supports PKCS#1 encoded RSA key lengths of 1024, 2048, and 4096 bits. Both SHA-1 and SHA-256 are supported as certificate integrity algorithms. The TOE supports [ConfigMode] 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 supported as an option. IPSec ESP is performed in tunnel mode in accordance with RFC 2406, 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. HMAC-SHA-1-96 is always used as the algorithm for producing message authentication codes. 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]. In addition, the TOE supports a proprietary TCP-based *Visitor Mode* tunneling protocol that

©2012 Check Point Software Technologies Ltd. All Rights Reserved.

Classification: [Unrestricted]—For everyone

Component	Description of mechanism
	allows remote access VPN clients to tunnel IKE and ESP over a single TCP port (e.g. 443).
FCS_CKM.2 /TLS, FCS_COP.1 /Admin, FCS_COP.1 /3DES , FCS_COP.1 /Hash, FCS_COP.1 /Signature	The TOE supports the TLSv1.0 secure channel protocol, in accordance with [RFC2246]. TLSv1.0 is used for three purposes: remote access SSL VPN, Secure Internal Communications (SIC) between TOE components, and for SmartDefense Updates. 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. SmartDefense Updates are downloaded over a TLS session established with the TLS_DHE_RSA_WITH_AES_256_CBC_SHA ciphersuite. VSX gateways support remote access SSL VPN by allowing a remote user to connect to a Virtual System over a Visitor Mode tunnel, and establishing a TLSv1.0 session with the VS. The same digital signature and password-based authentication mechanisms used for IPSec VPN are used for TLS client and gateway authentication. Each CMA contains an internal certificate authority (ICA) as described in section 1.5.3.11. The ICA generates X.509v3 certificates that are used for internal communications between the CMA and managed virtual entities, as well as with external clients using OPSEC APIs. Both SHA-1 and SHA-256 are supported as certificate integrity algorithms. In addition, the MDS contains its own ICA, used for issuing authorized administrator certificates and for MDS and CMA certificates. The ICA supports PKCS#1 encoded RSA, with key lengths of 1024, 2048 and 4096 bits. SHA-256 is used as the hash function. 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	The authorized System administrator associates VSX gateway logical interfaces with Virtual System, Virtual Router, and Virtual Switch entities. When an IPv4 packet is received by the gateway, it is labeled with a VSID in accordance with FDP_ITC.2, and processed by the corresponding Virtual System in accordance with FIA_USB.1 /IFF. Packet Inspection can result in either blocking the packet, or passing it through (modified or unmodified). Each VS maintains its own VRF tables, in which only its associated (physical, logical, and Warp) interfaces are registered. Therefore, the packet 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.

©2012 Check Point Software Technologies Ltd. All Rights Reserved.

Classification: [Unrestricted]—For everyone

Component	Description of mechanism
FDP_IFC.1 /TFF, FDP_IFF.1 /TFF	Information flow mediation is described in section 1.5.3.3 and 1.5.3.4. Every IPv4 packet received by the Check Point VSX 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 labeled with the VSID, 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 System administrator for the relevant Virtual System. 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. Every IPv4 packet that is allowed by the Packet Inspection capability is fed through a second set of Post-Inspect rules that attempt to match the packet against sets of attack signatures that may be installed by an authorized System administrator (SmartDefense Updates). 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 1.5.3.6. As described above for FDP_IFF.1 /TFF, ESP-encapsulated packets are processed in the VSX 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 Virtual System'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 administrator

©2012 Check Point Software Technologies Ltd. All Rights Reserved.

Classification: [Unrestricted]—For everyone

Component	Description of mechanism
	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 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 Virtual System's 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. The VPN Security Association is associated directly with the TCP session to the daemon. The VPN SFP is applied on inbound traffic before it is processed by the TRAFFIC FILTER SFP, and on outbound traffic after it is processed by the TRAFFIC FILTER SFP.
FDP_ITC.2	The TOE supports VLAN tagging in accordance with [802.1q], for both incoming and outgoing traffic. The SecurePlatform operating system on VSX 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 VSX gateway, Virtual System VSID 0 is modeled in the management GUI applications as corresponding to the VSX gateway object itself. By default, the VSID 0 security policy allows only TOE management traffic, dropping any other traffic.
FDP_RIP.2	When an incoming network frame is received by a Check Point VSX 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 Virtual System 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.
FDP_UCT.1 FDP_UIT.1	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, 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.

©2012 Check Point Software Technologies Ltd. All Rights Reserved.

Classification: [Unrestricted]—For everyone

Component	Description of mechanism
7.1.4. User identification and authentication (FIA)	
FIA_ATD.1	The MDS maintains a user database, containing accounts for administrators. Each account record contains the user's identity, supported authentication mechanisms, and association with an administrator role and a granular set of administrator authorizations, including Customer associations and group memberships. User certificates are stored in a separate ICA database. CMAs have read-only access to the MDS user and ICA databases for retrieving administrator account information. In addition, each CMA maintains a user database that contains non-administrator user accounts, for remote access VPN users. Each account record contains the user's identity and supported authentication mechanisms. Non-administrative user accounts are replicated to all CMA-managed Virtual Systems. Each CMA also maintains its own ICA database for storing non-administrative user certificates. 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 and Customer assignments are considered to be those of a. non-administrator.
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, TLS, 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 Provider-1 installation. Prior to authentication, Provider-1 does not allow any interaction with the administrator. A SIC-based trusted path is established between the management GUI and Provider-1. Administrator authentication is performed either via ICA-issued SIC certificates, or by configuring Provider-1 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 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

©2012 Check Point Software Technologies Ltd. All Rights Reserved.

Classification: [Unrestricted]—For everyone

Component	Description of mechanism
	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, RADIUS[25] authentication servers that may return authentication verdicts for single-use password authentication queries, and the Check Point Download Center Web site for downloading SmartDefense Updates. 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. The Check Point Download Center is authenticated by its TLS certificate.
FIA_UAU.7	All TOE interfaces that require entry of authentication data provide only obscured feedback to the user while the authentication is in progress.
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 /Admin	The MDS and CMA maintain active administrator sessions, and associate user identity, group memberships, authorisations and Customer associations for each session, by looking up the

[25] 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.

©2012 Check Point Software Technologies Ltd. All Rights Reserved.

Classification: [Unrestricted]—For everyone

Component	Description of mechanism
	authenticated administrator's account in the MDS user database. User-subject binding logic is as described in FIA_USB.1 /Admin. User identity is also recorded in all relevant audit records.
FIA_USB.1 /IFF	Binding of user to subject occurs on a VSX gateway when a packet is received for processing, and in Provider-1 for initiation of administration and OPSEC client sessions. User-subject binding logic is as described in FIA_USB.1 /IFF. The VSX 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 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. Authenticated remote access VPN users are associated with group memberships by looking up their account in the per-Virtual System local user database on the VPN gateway (see TSS FIA_ATD.1 entry above). User identity is also recorded in all relevant audit records.

7.1.5. Security Management (FMT)

FMT_MOF.1, FMT_MSA.1, FMT_MTD.1, FMT_SMF.1	As described in sections 1.5.3.9 and 1.5.3.10, TOE security management is performed using management GUI applications that connect to the Provider-1 installation. The authorized administrator role corresponds to administrators using the MDG or Global SmartDashboard GUI applications. The authorized System administrator role corresponds to administrators using the SmartConsole GUI applications. The OPSEC client role corresponds to users connecting to the TOE using non-TOE applications that use the client APIs described in section 1.5.3.12. As described for FTP_TRP.1 below, the TOE provides a trusted path for administration, using the Secure Internal Communications (SIC) facility. The administrator must authenticate to Provider-1 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. VSX gateways also receive management commands from Provider-1 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 therefore correspond to the functional capabilities of the interfaces used by each of the defined management roles. These are described in further detail in Table 7-3 below. 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 Functions**

Component	Management Function	Management Functionality
FMT_MOF.1	start-up and shutdown	VSX gateway start-up and shutdown are restricted to no administrator role because there is no

©2012 Check Point Software Technologies Ltd. All Rights Reserved.

Classification: [Unrestricted]—For everyone

Component	Description of mechanism		
			administrator interface that allows the authorized administrator to perform these actions. The authorized administrator can start-up and shutdown CMAs and MDSs from the MDG.
		create, delete, modify, and view default information flow security policy rules that permit or deny information flows globally for all Customers	The authorized administrator can define global policy rules using the Global SmartDashboard management GUI. Global rules are applied by the authorized administrator to all or selected CMAs. Each defined global rule can be either of higher priority than rules defined by the authorized System administrator (i.e. override the latter), or be of lower priority, thus presenting a default flow control that may be overridden through corresponding rules created by the authorized System administrator.
		create, delete, modify, and view information flow security policy rules that permit or deny information flows for Virtual Systems for a specific Customer	The authorized System administrator uses SmartDashboard, connected to a CMA, for managing information flow security policy for a specific Customer.
		create, delete, modify, and view user attribute values defined in FIA_ATD.1 for administrator roles	Administrator accounts and administrator SIC certificates are managed by the authorized administrator using the MDG.
		create, delete, modify, and view user attribute values defined in FIA_ATD.1 for non-administrators	Non-administrator user accounts are managed by the authorized System administrator using SmartDashboard.
		enable and disable single-use authentication mechanisms in FIA_UAU.4	SIC certificates for administrators are managed by the authorized administrator from the MDG. Authentication of VPN peers is configured by the authorized System 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. The authorized administrator can configure global VPN security attributes using the Global SmartDashboard management GUI.

©2012 Check Point Software Technologies Ltd. All Rights Reserved.

Classification: [Unrestricted]—For everyone

Component	Description of mechanism		
			Shared secrets 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 System administrator in the RADIUS server objects in the SmartDashboard Objects Database. An authorized System 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.
		modify and set the time and date	There is no administrator interface for modifying the clock once the TOE is operational.
		archive, create, delete, and empty the audit trail	The SmartView Tracker management GUI allows the authorized System 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.
		review the audit trail	The SmartView Tracker management GUI allows authorized System administrators and authorized administrators 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 1.5.3.12). LEA is a well-defined API that 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 to no administrator role when the TOE is operational, as there is no management GUI interface that supports these operations. Backup can be scheduled during installation and generation of

©2012 Check Point Software Technologies Ltd. All Rights Reserved.

Classification: [Unrestricted]—For everyone

Component	Description of mechanism		
		recover to the state following the last backup	the TOE, and restoration can be performed from a previously performed backup during installation and generation of the TOE. SmartView Tracker can be used to export audit trail data for backup purposes.
		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	MDG allows the authorized administrator to specify addresses from which management GUIs can connect to the Provider-1 installation. This applies to both local and remote administration. Information security policy rules created by the authorized System administrator in SmartDashboard can further restrict possible remote administration addresses.
		modify the behaviour of the functions of System data collection, analysis and reaction	SmartDashboard allows the authorized System administrator to define information flow control rules and IDS/IPS behavior that control System data collection, analysis and reaction. The authorized administrator can also load SmartDefense Updates through the SmartDashboard management GUI.
		enabling SIC trust between Provider-1 and a VSX gateway	Enabling SIC connectivity between a CMA and a VSX gateway is performed during installation and generation of the gateway, in conjunction with corresponding definitions entered by an authorized System administrator in the SmartDashboard management GUI.
	FMT_MSA.1	query, modify Virtual System interface and Customer associations	An authorized System administrator manages Virtual Systems and interface allocations using the SmartDashboard management GUI.
	FMT_MTD.1	query IDS System and audit data	The SmartView Tracker management GUI allows the authorized System administrator and authorized 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 1.5.3.12). LEA is a well-defined API that provides log record information, including a data dictionary that assists the application in interpreting the

©2012 Check Point Software Technologies Ltd. All Rights Reserved.

Classification: [Unrestricted]—For everyone

Component	Description of mechanism		
			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 authorized administrators and authorized System administrators 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 allows the authorized System administrator to define thresholds for required free disk space and to enable the generation of an Alert when the threshold is exceeded. VSX gateway fail-safe behavior in the event of storage exhaustion is configured using SmartDashboard.
FMT_MSA.3 /MAC	An authorized System 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_MSA.3 /IFF	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 global rules that allow authenticated management traffic between VSX gateways and Provider-1 hosts. Evaluated configuration guidance recommends that these rules be configured by the authorized administrator using the Global SmartDashboard management GUI. Any other information flows are denied by default. The authorized administrator can override these default rules.		
FMT_REV.1 /Admin	The authorized administrator manages administrator accounts using the MDG. In order to revoke user security attributes, the administrator must have revocation authorisations. An administrator session is associated with roles and authorizations during session initiation. Modifications to administrator authentication information, roles and privileges are applied in the MDS user database, and will immediately become applicable to the administrator's next login. If the administrator is already logged-in, the authorized administrator can disconnect his session immediately from the *Connected Administrators* view in MDG.		
FMT_REV.1 /User	Non-administrator user accounts are managed by the authorized System administrator from SmartDashboard. Other user or roles cannot revoke user security attributes. In order to revoke user security attributes, the administrator must have revocation authorisations. Non-administrator users connect to VSX gateways. The CMA-managed user databases are replicated to the gateways, so that the relevant Virtual Systems can authenticate users without		

©2012 Check Point Software Technologies Ltd. All Rights Reserved.

Classification: [Unrestricted]—For everyone

Component	Description of mechanism
	having to query the CMA. Modifications to a user account will become applicable on the gateway immediately upon security policy installation by an authorized System administrator.
FMT_SMR.1	The definition of the authorized administrator and authorized System administrator in the context of this ST is given in section 1.5.3.10. OPSEC client APIs are identified in section 1.5.3.12.

7.1.6. Protection of the TSF (FPT)

FPT_FLS.1	During initial start-up of a VSX 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 VSX 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[26] are protected from disclosure and modification by the Secure Internal Communications (SIC) security function. SIC protects all communications between management GUIs and Provider-1, communications between multiple Provider-1 hosts, and communications between Provider-1 hosts and managed gateways. SIC incorporates the TLSv1.0 protocol, using AES encryption and RSA digital signatures for authentication (see above for FCS_CKM.2 /TLS). As described in section 1.5.3.11, 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 VSX gateways and Check Point Provider-1 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 Provider-1 CMA; 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 MD5-based single-use authenticators as defined in the NTP protocol ([RFC1305]). 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

[26] 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.

©2012 Check Point Software Technologies Ltd. All Rights Reserved.

Classification: [Unrestricted]—For everyone

Component	Description of mechanism
	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 MDS hosts. MDS configuration object changes are replicated immediately. MDS ICA and global policy information is replicated when a new policy is saved and/or on a predefined schedule. CMA databases can be replicated from an active CMA to zero or more standby CMAs installed on other MDS hosts. All Customer-specific management operations such as editing and installing the Security Policy and modifying users and objects, are performed against the active CMA. If the active CMA is unavailable, one of the standby CMAs should be made active. This transition from standby to active is initiated manually by the authorized administrator. Log records are not replicated between CMAs. In order to allow log review on both active and standby CMAs, VSX gateways can be configured to forward log records to multiple CMAs. The administrator installs the security policy on the VSX cluster rather than separately on individual cluster members. The policy is automatically installed on all VSX 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 CMA for each VS. If the policy on the CMA is more up to date than the one on the cluster member, the policy on the CMA will be retrieved. If the cluster member does not have a local policy, it retrieves one from the CMA. This ensures that all cluster members use the same policy at any given moment. 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. 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 VSX 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 VSX gateway, and comparing it to a stored value. Policy files are verified when they are received from the CMA 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 VSX 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. Administrators can determine that managed appliances are in operational status via the SmartView Monitor Management GUI.

©2012 Check Point Software Technologies Ltd. All Rights Reserved.

Classification: [Unrestricted]—For everyone

Component	Description of mechanism
7.1.7. Fault tolerance (FRU)	
FRU_FLT.2	As described above for FPT_TST.1, VSX gateways perform self-tests for verifying 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 1.5.3.13. The cluster redirects subsequent packets to the newly active virtual entities. This ensures that all TOE capabilities are retained. TSF data stored in Provider-1 is replicated between all MDS hosts, as described above for FPT_TRC.1. If a failure of a critical hardware or software entity occurs, administrators can continue working with a backup host with no loss of functionality.
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 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 CMA or MDS, 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 1.5.3.5, the TOE's claimed intrusion detection analysis functionality is implemented using Check Point's INSPECT Stateful Inspection virtual machine engine. Network traffic that has been allowed by the firewall and VPN security policies is compared against signature events encoded in INSPECT language. INSPECT is an object-oriented, high-level, loop-free script language that specifies packet handling by classifying packet content and state. INSPECT scripts are compiled by a Provider-1 installation into low-level inspection code that is executed on VSX 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 a 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 TSP. Encoded signature events can be set to log the detected potential violation. INSPECT matching is performed twice: during Packet Inspection and during Post-Inspect (see below for FDP_IFF.1 /TFF). An authorized System administrator can set up IDS signature events using both capabilities; by setting up a Packet Inspection rule that matches the defined

©2012 Check Point Software Technologies Ltd. All Rights Reserved.

Classification: [Unrestricted]—For everyone

Component	Description of mechanism
	signature and reacts accordingly, or by loading a canned set of signature events that will be matched during Post-Inspect. Check Point VSX gateways record within each analytical result (manifested as a match against an INSPECT rule) the following information required by IDS_ANL(EXP).1: date and time of the result, type of result (rule number matched), and identification of data source (source IP address). In addition, the identity of the Virtual System that generated the log record is recorded within the result.
IDS_RCT(EXP).1	When an intrusion is detected, i.e. when incoming traffic matches an IDS signature encoded in INSPECT language, the authorized System administrator configures the Packet Inspection rules to log the event and/or drop the suspected traffic. Auditable events are configured by the authorized System 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 CMA log database. Administrators review the logs in human readable form using SmartView Tracker. As described above for FAU_SAR.1, both authorized System administrators and authorized OPSEC clients may connect to a CMA and review audit trail data, constrained by the user's authorisations and Customer assignments. IDS System data is not forwarded to the MDS, and is therefore not accessed by the authorized administrator role. As described above for FAU_SAR.2, the Provider-1 installation restricts access to 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 CMA log database. The VSX 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 INSPECT rules). For each event, the audit record contains the following information required by IDS_SDC(EXP).1: date and time of the event, type of event (rule number matched), subject identity (presumed source IP address), the outcome of the event (accept, drop, or reject), and in addition: protocol, service, and destination address. For detected known vulnerabilities, the identification of the 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 CMA 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. VSX 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.

©2012 Check Point Software Technologies Ltd. All Rights Reserved.

Classification: [Unrestricted]—For everyone

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 VSX gateway, that prevents any external access to these components.

Virtual Systems are described in section 1.5.3.2. Virtual Systems process incoming packets as described for the information flow control policies above. Each packet and all associated information is labeled with the VSID, so that it is processed in the context of its binding with a specific Virtual System. VS binding and transfer of packets between VSs is described in FIA_USB.1.

Because the VSID is universal across VSX cluster members, VSID-based information separation is maintained when state tables are synchronized.

Each Virtual System maintains its own topology definitions, including interface associations, interface address ranges, virtual routing and forwarding tables (VRFs), and ARP tables. The TSF uses these definitions when forwarding packets between Virtual Systems and to external interfaces. Information flows between VSs only through physical, logical, or Warp interfaces.

Each Virtual System also maintains separate policy and log file directories on the VSX gateway, and establishes an independent SIC trusted channel to its manager CMA, based on a per-VS RSA private key and corresponding ICA certificate, issued by the CMA.

Each CMA maintains separate security policy, user database, and log database directories on the Provider-1 installation. Management high-availability replication can be configured only between CMAs that are associated with the same Customer, on separate MDS hosts. Authorized System administrators connect directly to the CMA; therefore, this is no leakage of information between CMAs. An authorized System administrator can only gain access to information belonging to Customers that he is assigned to.

The MDS communicates with its CMAs, e.g. for global policy updates. However, the MDS does not collect any controlled information from its managed CMAs (i.e. policy information, logs, traffic) and so inter-CMA separation is maintained.

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.

©2012 Check Point Software Technologies Ltd. All Rights Reserved.

Classification: [Unrestricted]—For everyone

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 VSX 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 kernel thread verifies the existence of critical processes. CPU, memory and disk resources are monitored continuously and can be displayed using the SmartView Monitor management GUI.

Policy files are verified by the VSX gateway when they are received from the CMA. Software integrity is verified during startup. Administrators can determine that managed appliances are in operational status via the SmartView Monitor management GUI.

©2012 Check Point Software Technologies Ltd. All Rights Reserved.

Classification: [Unrestricted]—For everyone

7.3. Protection against Bypass

7.3.1. Virtual Defragmentation

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

7.3.2. Residual Information Protection

All buffers containing Customer-specific information are cleared before being allocated to a Virtual System, thus preventing residual information from leaking between security domains.

All buffers containing packet information and cryptographic keying material are cleared before being reallocated.

7.3.3. Boot Security

During the Check Point VSX 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 VSX gateway is in an operational state.

Each Virtual System maintains its own separate policy rule base, logs, state tables, networking definitions, and SIC identity. Packets received by the gateway are bound to a VS in accordance with the logical interface over which they are received, and are processed in that context. An external user cannot bypass packet inspection or cause information to flow to another Customer's interface except through defined virtual networking entities.

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.

©2012 Check Point Software Technologies Ltd. All Rights Reserved.

Classification: [Unrestricted]—For everyone

8. Supplemental Information

8.1. References

The following external documents are referenced in this Security Target.

Identifier	Document
[802.1Q]	Virtual Bridged Local Area Networks, IEEE Std 802.1Q, 2003 Edition, May 2003
[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
[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
[802.1q]	*IEEE Standard for Local and metropolitan area networks – Virtual Bridged Local Area Networks*, IEEE Std 802.1Q-2005, 19 May 2006.
[IDSSPP]	U.S. Government Protection Profile Intrusion Detection System System for Basic Robustness Environmemts, Version 1.7, July 25, 2007

©2012 Check Point Software Technologies Ltd. All Rights Reserved.

Classification: [Unrestricted]—For everyone

[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),

©2012 Check Point Software Technologies Ltd. All Rights Reserved.
Classification: [Unrestricted]—For everyone

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

[RFC2560] RFC 2560 – X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP, June 1999

[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

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

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

[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

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

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

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

©2012 Check Point Software Technologies Ltd. All Rights Reserved.
Classification: [Unrestricted]—For everyone

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.SYSTEM".
- Subjects are denoted by the prefix "S.", e.g. "S.CMA".
- 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. "/MAC". These follow the short family name and allow components to be used more than once with varying operations.

©2012 Check Point Software Technologies Ltd. All Rights Reserved.

Classification: [Unrestricted]—For everyone

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.

©2012 Check Point Software Technologies Ltd. All Rights Reserved.

Classification: [Unrestricted]—For everyone

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[27] 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.

[27] This is an example of a footnote.

©2012 Check Point Software Technologies Ltd. All Rights Reserved.

Classification: [Unrestricted]—For everyone

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], [CAPP]. 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: *6.2.7.4. Audit review (FAU_SAR.1)* FAU_SAR.1.1 The TSF shall provide **authorized roles defined in FMT_SMR.1** with the capability to read **all audit trail data** from the audit records.	(completed) Assignment
Underline	Underlined text denotes completed component selections (out of a set of selection options provided in the original CC requirement). Example: *6.2.9.1. Basic internal TSF data transfer protection (FPT_ITT.1)* FPT_ITT.1.1 The TSF shall protect TSF data from disclosure and modification when it is transmitted between separate parts of the TOE.	(completed) Selection
Boldface Underline	Underlined boldface text highlights component refinements. This includes refinement of an operation that was completed in the PP. Example: *6.2.8.4. Static attribute initialization (FMT_MSA.3 /IFF)* FMT_MSA.3.1 The TSF shall enforce the **TRAFFIC FILTER SFP** to provide restrictive default values for information flow security attributes that are used to enforce the SFP.	Refinement

©2012 Check Point Software Technologies Ltd. All Rights Reserved.

Classification: [Unrestricted]—For everyone

Convention	Purpose	Operation
Slash (iteration name)	A slash and an iteration nameinform the reader that the requirement component will be used multiple times. Examples: *6.2.5.1. Subset information flow control (FDP_IFC.1 /TFF)* FDP_IFC.1.1 The TSF shall enforce the TRAFFIC FILTER SFP on:… *6.2.5.2. 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: *6.2.11.2. Analyzer react (IDS_RCT(EXP).1)* IDS_RCT(EXP).1.1 The System shall send an alarm…	Extended Requirement

©2012 Check Point Software Technologies Ltd. All Rights Reserved.

Classification: [Unrestricted]—For everyone

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 VSX 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[28] and the disclosure and modification of data.[29]

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.

Audit trail A log of recorded security-relevant events in the TOE.

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.

[28] Hardware and software.

[29] Stored or communicated.

©2012 Check Point Software Technologies Ltd. All Rights Reserved.

Classification: [Unrestricted]—For everyone

Authorised user	An authenticated user who may, in accordance with the TSP, perform an operation.
Availability	Timely[30], reliable access to IT resources.
Bridge	A networking device that forwards frames between LANs.
ClusterXL	A Check Point clustering technology.
Compromise	Violation of a security policy.
Confidentiality	A security policy pertaining to disclosure of data.
Cryptographic key (key)	A parameter used in conjunction with a cryptographic algorithm that determines: • the transformation of plaintext data into cipher text data, • the transformation of cipher text data into plaintext data, • a digital signature computed from data, • the verification of a digital signature computed from data, or • a digital authentication code computed from data.
Customer	A business entity that owns a set of Virtual Systems (and connected enclaves), managed by a single CMA.
Customer Management Add-On	A software component of the Provider-1 installation that provides security policy management for a single Customer domain.
Dynamic Routing	Routing of IP packets based on a dynamically-calculated network topology based on route update messages exchanged between routing gateways.
Enclave	Collection of computing environments connected by one or more internal networks under the control of a single authority and security policy.
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.
IEEE 802.1q	A VLAN standard for tagging layer-2 frames.

[30] According to a defined metric.

©2012 Check Point Software Technologies Ltd. All Rights Reserved.

Classification: [Unrestricted]—For everyone

INSPECT	A patented Check Point virtual machine for stateful inspection.
Integrity	A security policy pertaining to the corruption of data and TSF mechanisms.
Multi-Domain GUI	A management GUI application used to manage Provider-1.
Named Object	An object that exhibits all of the following characteristics: • The object may be used to transfer information between subjects of differing user identities within the TSF. • Subjects in the TOE must be able to request a specific instance of the object. • The name used to refer to a specific instance of the object must exist in a context that potentially allows subjects with 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.
Router	A layer-3 device that routes packets based on information in the IP header and static or dynamic topology information.
Routing Protocol	A network protocol used to exchange router topology updates.

©2012 Check Point Software Technologies Ltd. All Rights Reserved.

Classification: [Unrestricted]—For everyone

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.

SmartConsole A set of integrated management GUI applications including SmartDashboard, SmartView Tracker, and SmartView Monitor.

SmartDashboard A management GUI used by authorized System administrators.

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

SmartDefense Update

The capability to load IDS/IPS attack signature updates.

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

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

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.

System data A term introduced by [IDSSPP], referring to information collected from the targeted IT System resource(s).

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.

©2012 Check Point Software Technologies Ltd. All Rights Reserved.

Classification: [Unrestricted]—For everyone

User	Any entity (human user or external IT entity) outside the TOE that interacts with the TOE.
Virtual LAN	A logical partition of a LAN, created using 802.1q tagging.
Virtual Router	A virtual VSX junction that routes packets between Virtual Systems and interfaces.
Virtual Switch	A virtual VSX junction that forwards packets between Virtual Systems and interfaces.
Virtual System	A logical instance of an information flow control subject running on a VSX gateway.
VPN domain	The set of addresses defined to be 'internal' in a Virtual System's topology.
Vulnerability	A weakness in the TOE that can be used to violate the SFRs in some environment.
Warp Link	An association between a Virtual System and a Virtual Router or Virtual Switch.

©2012 Check Point Software Technologies Ltd. All Rights Reserved.

Classification: [Unrestricted]—For everyone

8.3.2. Abbreviations

Abbreviation	Description
AES	Advanced Encryption Standard
API	Application Programming Interface
ARP	Address Resolution Protocol
BGP	Boundary Gateway Protocol
CA	Certificate Authority
CC	Common Criteria
CCIMB	Common Criteria International Management Board
CLI	Command Line Interface
CM	Configuration Management
CMA	Customer Management Add-on
CRL	Certificate Revocation List
CRL DP	Certificate Revocation List Distribution Point
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

©2012 Check Point Software Technologies Ltd. All Rights Reserved.

Classification: [Unrestricted]—For everyone

Abbreviation	Description
IP	Internet Protocol
IPS	Intrusion Prevention System
IPSec	Internet Protocol Security
IT	Information Technology
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
MAC	Message Authentication Code
MDS	Multi-Domain Server
MDG	Multi-Domain GUI
MD5	Message Digest 5
NAT	Network Address Translation
NIC	Network Interface Card
NTP	Network Time Protocol
OCSP	Online Certificate Status Protocol
OPSEC	Open Platform for Security
OS	Operating System
OSP	Organizational Security Policy
OSPF	Open Shortest Path First
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

©2012 Check Point Software Technologies Ltd. All Rights Reserved.

Classification: [Unrestricted]—For everyone

Abbreviation	Description
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
SPI	Security Parameter Index
SSH	Secure Shell
SSL	Secure Sockets Layer
ST	Security Target
STP	Spanning Tree Protocol
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
VSID	Virtual System Identity

.

©2012 Check Point Software Technologies Ltd. All Rights Reserved.

Classification: [Unrestricted]—For everyone

Appendix A - TOE Hardware Platforms

A.1. Supported Hardware for VSX Gateways

The following hardware platforms are included in the evaluated configuration for the security policy enforcement software (VSX gateways), running the Check Point SecurePlatform VSX operating system.

This evaluation considers the hardware to be self-contained, providing no remote access to any of the hardware resource that might bypass the NIC interface and the operating system (e.g. shared disks, remote console interfaces, Lights Out Management, virtualized network interconnects, etc.). All supported platforms provide the operating system with direct access to the hardware.

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[31]
- **Memory**: a minimum of 512 Mbytes
- **Mass Storage**: a minimum of 9 GBytes
- **Network controllers**: the following adapter families are included:

Chipset	Driver	Included Adapters
Intel® 825xx	e100	Any adapter from the Intel® Pro/100 family
	e1000, 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

[31] Check Point FIPS 140-2 testing was performed on single and dual Intel Xeon and AMD Opteron configurations. FIPS 140-2 Implementation Guidance G.5 allows vendor porting and re-compilation of a validated firmware cryptographic module to a processor configuration that was not included as part of the validation testing, when this does not require source code modifications. The validation status is maintained in this case without re-testing.

©2012 Check Point Software Technologies Ltd. All Rights Reserved.

Classification: [Unrestricted]—For everyone

- **Platforms**:

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

A.2. Supported Check Point Security Appliances

The following Check Point security appliance models are included in the evaluated configuration for the security policy enforcement software (gateways):

- VSX-1 3070
- VSX-1 9070
- VSX-1 9090
- VSX-1 11000 series
- VSX-1 11200 series (VSLS)
- Check Point 12200 VSX
- Check Point 12400 VSX
- Check Point 12600 VSX
- Check Point 21400 VSX

These appliances run Check Point VSX R67.10.20, on an appliance-specific build of the Check Point SecurePlatform VSX R67.10.20 operating system.

©2012 Check Point Software Technologies Ltd. All Rights Reserved.

Classification: [Unrestricted]—For everyone

A.3. Supported Hardware for Provider-1

The following hardware platforms are included in the evaluated configuration for Provider-1, running the Check Point SecurePlatform R71 with R7x hotfix 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®, Intel Pentium® IV, Intel XEON® processor configurations, minimum 2 GHz
  - Other processors that are code-compatible with the listed configurations
- **Memory**: a minimum of 4 Gb
- **Mass Storage**: a minimum of 10 Gb (installation includes operating system) for the MDS plus 100 Mb for each CMA.
- **Platforms**:
  - The platforms listed in section A.1 above; and
  - The following Check Point security appliance models:
    - Smart-1 50
    - Smart-1 150

©2012 Check Point Software Technologies Ltd. All Rights Reserved.

Classification: [Unrestricted]—For everyone