
SmartUse Sample Report

Customer: Alice & Bob inc

Customer Contact: John Doe

Customer E-mail: jdoe@alicenbob.com

Report Period: Q1 2010

Date of Data Collection: March 15th-19th 2010

Report Date: April 10th, 2010

Check Point Consultant: Eran Ashkenazi

This report is a **sample report.
The Report content may vary based on the client's
deployment and our findings.**

The report is available on the web:

<http://www.checkpoint.com/services/smartsuse/index.html>

Disclaimer

Recommendations in this report are best practice recommendations given by Check Point experts. The recommendations are based on data collected by the customer contact on the Report Date and are considered a good representation of the customer's regular network usage.

Each recommendation is rated as follow:

























-  Serious – Needs immediate attention.
-  Attention – Needs attention.
-  Good - No need for any action.



Table of Contents

1. EXECUTIVE SUMMARY	3
GOAL	3
FINDINGS	3
2. SECURITY AND STABILITY	4
2.1. SMARTDEFENSE PROTECTIONS	4
2.1.1. <i>Activate SmartDefense Protections</i>	4
2.1.2.  <i>Download SmartDefense Protections</i>	4
2.2. RULE BASE IMPROVEMENTS	5
2.2.1.  <i>Anti-Spoofing Configuration</i>	5
2.2.2.  <i>Rule Base Security Improvements</i>	6
2.2.3.  <i>Stealth and cleanup rule</i>	7
2.2.4.  <i>Additional Rule Base Recommendations</i>	7
2.3.  GLOBAL PROPERTIES	8
2.4.  VPN COMMUNITIES	9
2.5.  DATABASE INTEGRITY	9
3. RULE BASE PERFORMANCE IMPROVEMENTS.....	9
3.1.  MOST ACTIVE RULES	9
3.2.  LEAST ACTIVE RULES.....	10
3.3.  UNUSED RULES.....	10
3.4.  CONSOLIDATE RULES.....	10
3.5.  UNUSED OBJECTS	11
3.6.  DUPLICATED OBJECTS.....	11
3.7.  NESTED GROUPS.....	11
4. ADDITIONAL RECOMMENDATIONS	12
4.1.  ADMINISTRATOR CLEANUP	12
4.2.  OPERATING SYSTEM SERVICE PACK AND PATCHES	12
4.3.  MEMORY USAGE.....	12
4.4.  DISK SPACE.....	13
4.5.  SUPPORT CONTRACT STATUS	13
4.6.  AVAILABLE HFA.....	13



1. Executive Summary


Goal

The goal of this review was to closely examine the deployment of your Check Point products, and assert what can be done to optimize network security management – both in terms of security best practices and of performance optimization. To achieve this, information about your Check Point products with a focus on your SmartCenter Server was analyzed using a multitude of utilities. These utilities enabled us to discover issues in your environments that require attention.

Findings

After a complete analysis, the following issues were discovered:

-  4 Serious
-  11 Attention
-  6 Good

The following  Serious issues were discovered as a result of our analysis of your deployment:

[Activate SmartDefense Protections](#)

[Stealth and Cleanup Rule](#)

[Most Active Rules](#)

[Available HFA](#)



2. Security and Stability

2.1. SmartDefense Protections

2.1.1. Activate SmartDefense Protections

After analyzing your deployment, policy and traffic, we have found that important SmartDefense and Web Intelligence protections are inactive.

Important note:

You should backup your SmartDefense (SD) profile before making any change to it.

To backup your SmartDefense current profiles:

1. Go to SmartDashboard -> SmartDefense Tab -> Profile Management
2. Select the SD profile that you want to backup.
3. Click on "New..." button -> Clone Selected Profile
4. Then enter a name for the SD backup profile -> Click "OK" button
5. VSX supports only the default profile and might support only some of the protections mentioned below.

Within the listed information of the discovered gateways, each with its security policy which holds a specified SmartDefense profile is the list of protections which should be activated for the profile.

To improve your network's security, you should consider activating the following SmartDefense and/or Web Intelligence Protections (protections with performance hit marked in **red**):

For policy package: **Extrior_FW**, SD profile: **Smart defense profile**, gateways: **Gateway**

- SmartDefense-->Network Security-->Fingerprint scrambling-->ISN spoofing
- SmartDefense-->Network Security-->Fingerprint scrambling -->TTL
- SmartDefense-->Network Security-->TCP-->Small PMTU
- SmartDefense-->Network Security-->TCP-->spoofed reset protection
- SmartDefense-->Application Intelligence-->DNS-->domains block list
- SmartDefense-->Application Intelligence-->DNS-->mismatched replies
- SmartDefense-->Application Intelligence-->DNS-->scrambling

2.1.2. Download SmartDefense Protections

Your SmartDefense protections were last updated on Dec 13th 2006. It looks like you never updated your SmartDefense protections, either because you are not subscribed or because you didn't know the option exist.

The following is a list of **critical and high level** protections that are available in Check Point's web site and are not installed on your system:



Severity	Date	Check Point Reference	Industry Reference	Description
Critical	02-Mar-10	CPAI-2010-049	CVE-2010-0483	Update Protection against Microsoft VBScript MsgBox Call with Malicious HLP File Vulnerability
Critical	01-Mar-10	CPAI-2010-040	CVE-2010-0242	Update Protection against Microsoft Windows TCP/IP Selective Acknowledgement Denial of Service Vulnerability (MS10-009)
Critical	24-Feb-10	CPAI-2010-039	CVE-2010-0186	Update Protection against Adobe Flash Player Subvert Domain Sandbox Vulnerability (APSB10-06)
Critical	24-Feb-10	CPAI-2010-038		Update Protection against the Kneber/Zeus Botnet
Critical	19-Feb-10	CPAI-2010-111	CVE-2009-3999	Update Protection against HP Power Manager formExportDataLogs Buffer Overflow
High	19-Feb-10	CPAI-2010-110		Update Protection against Oracle TimesTen In-Memory Database HTTP Request Denial of Service
Critical	19-Feb-10	CPAI-2010-109		Update Protection against Sun Java System Web Server Digest Authorization Buffer Overflow

To see a full list of SmartDefense protections refer to:
<http://www.checkpoint.com/defense/advisories/public/index.html>

2.2. Rule Base Improvements

The rule base contains several rules that can be modified to enhance security and performance.

2.2.1. Anti-Spoofing Configuration

Anti Spoofing is configured properly on all Gateways



2.2.2. Rule Base Security Improvements

Possible Risk: The following active rules pose a potential security risk. Our recommendations for rule modifications target accept rules that have misuse of “Any” in the source, destination or service column.

Policy Package: Exterior_FW

Rule: 19, 27, 59

NO.	Source	Destination	VPN	Service	Action	Track
19	Configuration-Manager	Internal_servers	Any	Any	accept	Log
27	Any	DMZ_net	Any	Any	Accept	Log
59	Partner_net_1, Partner_net_2	Auth_server	Any	Any	Accept	Log

Solution: The following list shows the result of our analysis of your logs, consider using these **services** separately or in a service group instead of using “Any”:

Rule	Gateway	Services
19	CP_perimiter	tcp/80, tcp/8080, tcp/21, tcp/20, tcp/443, tcp/4433, tcp/902, tcp/903
	CP_internal	tcp/5050, tcp/88, tcp/80, tcp/443, tcp/563
27	CP_perimiter	N/A
	CP_internal	tcp/22, udp/53
59	CP_perimiter	tcp/49, udp/53, udp/1645, udp/1646,
	CP_internal	N/A

Possible Risk: Possible Risk: The following active rules pose a potential security risk. Our recommendations for rule modifications will fix the policy for enhanced security Rules that have 'any' in the source column and 'accept' in the action column

Policy Package: Exterior_FW

Rule: 31

NO.	Source	Destination	VPN	Service	Action	Track
31	Any	NOV_Surfing_192.168.9.0, Houston-TX-PWC-Surf	Any	telnet, http_https, ssh	accept	Log

Solution: The following list shows the result of our analysis of your logs, consider using these **sources** separately or in a network object group instead of using “Any”:

Rule	Gateway	Sources
31	CP_perimiter	232.41.163.32, 202.45.193.38, 125.174.120.243, 155.22.15.31, 155.22.15.37, 155.22.15.38
	CP_internal	101.33.225.22, 232.41.163.32, 202.45.193.29, 133.196.111.107



Possible Risk: Rules in each policy with icmp-proto protocol

Policy Package: Exterior FW







Rule: 61

NO.	Source	Destination	VPN	Service	Action	Track
61	Internal Networks	Any	Any	icmp-proto	accept	Log

Solution: 'icmp-proto' consists of many unsafe protocols. If you want to allow the ability to ping consider changing the service to 'echo-request'.

2.2.3. Stealth and cleanup rule

You have no stealth rule in place in the “Exterior FW” policy package. The stealth rule is an essential part of your security policy to prevent abuse to your security gateways.

Policy Package	Stealth Rule	Cleanup Rule
Edges		
Exterior FW		
Internal FW		


You should install a stealth rule in the “Exterior FW” policy package.

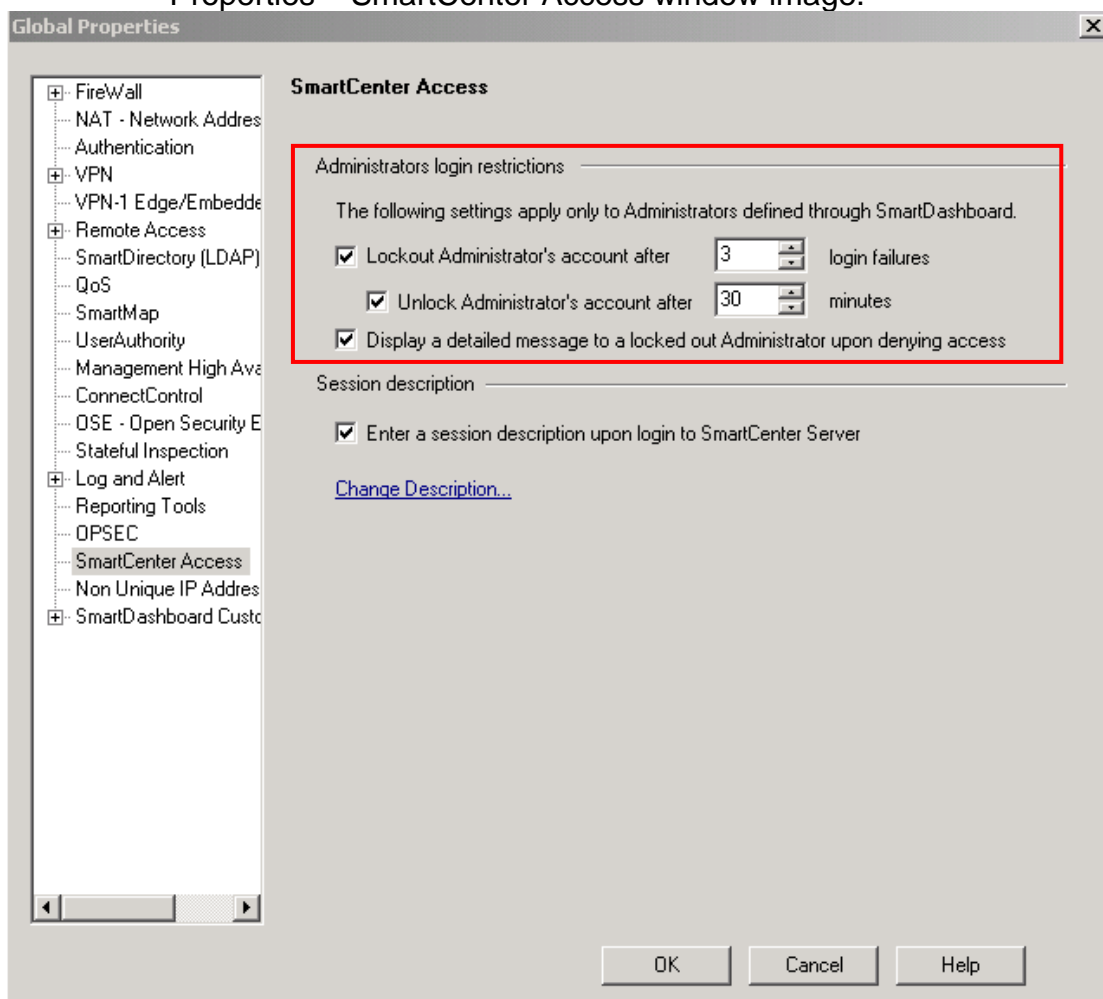
2.2.4. Additional Rule Base Recommendations

You are currently using a stealth rule (which is good), but it's recommended to log it for forensic and in order to watch anomalies. Usually there should be not much logs in this rule unless you are under attack.



2.3. Global Properties

- 2.3.1.  SmartCenter Access – no lockout administrator policy is selected. Consider enabling the lockout option as shown in the following Global Properties – SmartCenter Access window image.



2.4. VPN Communities

The following is a list of VPN keys that can be configured for better performance of your system. We recommend that you change your algorithm strength accordingly.

Community Name	IKE Phase I	IKE Phase II	Recommendation
RemoteAccess	3DES/MD5	AES-128/MD5	Consider changing the integrity to SHA1. Consider changing Phase I encryption to AES-256.
NY-SF-offices_VPN	DES/SHA1	AES256/SHA1	Consider changing Phase I encryption to AES-256. In case performance issues arise consider changing IKE phase II encryption algorithm to 3DES

2.5. Database Integrity

No errors were found.

An upgrade to R70 was performed successfully without problems.

3. Rule Base Performance Improvements

3.1. Most Active Rules

The following rules are the most active rules

Solution: Consider moving them to the top of the rule base – based on your deployment and security architecture.

Top Matched Logged Rules (Policy: Extrior_FW)		
Rule Number in Current Policy	Number of Connections	% of Total Connections
240	73,439	66.83%
179	16,933	15.41%
434	7,975	7.26%
23	5,596	5.25%



3.2. **Least Active Rules**

The following rules are the least active rules

Solution: Consider moving them towards the bottom of the rule base – based on your deployment and security architecture.

Least Matched Logged Rules (Policy: Extrinsic_FW)		
Rule Number in Current Policy	Number of Connections	% of Total Connections
8	968	0.97%
29	675	0.68%
34	142	0.14%
58	95	0.09%

3.3. **Unused Rules**

According to the log analysis the following rules have found to be not used.

Solution: Consider disabling them, and then gradually removing them from your rule base.

Policy Name	Rules
Extrinsic_FW	2, 15, 33, 39, 55, 99, 103, 274
Intrinsic_FW	5, 38, 115

3.4. **Consolidate Rules**

Policy Package: Local_Policy

Reason: Same source, same destination, but different service

NO.	Source	Destination	VPN	Service	Action	Track
133	Users@ Any	PC_10.105.100.74	RemoteAccess	MS_TerminalServer, VNC	accept	Log
139	Users@ Any	PC_10.105.100.74	RemoteAccess	Any	accept	Log



3.5. **Unused Objects**

The following objects are not being used.

Solution: Consider removing them.

Object Name	Object IP (if applicable)
ronda	172.145.43.75
Milano	192.164.121.47
Host1	10.163.141.56
Old_pc	226.200.149.175
NY_test2	
EXT-155.108.127.98	10.108.127.98

3.6. **Duplicated Objects**

The following objects are exactly the same.

Solution: Remove one of each pair of duplicates (verify the object you want to delete with "where used" prior to deletion).

Object Name	Duplicate Object Name	Object IP (if applicable)
Ny_sql	star	
HOST7	HOST-10.33.64.1	10.33.64.1
HOST-10.23.4.5	SF-Cal	10.23.4.5
NET-10.37.0.0_16	N10.37.0.0_16	

3.7. **Nested groups**

There are many object of type Group that contains other Groups as internal objects. You are strongly advised to use plain Groups and to refrain from using nested groups.

Nested group objects:

- John_doe_PCs
- Exchange_Servers (2 level of nested groups)
- DNS_Servers
- Malicious_Sources



4. Additional Recommendations

4.1. **Administrator Cleanup**

These are the administrators configured in your system make sure all administrators are allowed by company policy

- admin1
- admin2
- root1
- root2
- superroot
- reviewer1
- tempadmin

Please review this list and verify that only authorized users has access to the SmartCenter.

4.2. **Operating System Service Pack and Patches**

Your system is fully patched. No action is required.

4.3. **Memory usage**

The examination of the management's memory statistics resulted in the following (values are in KB):

	Total	Used	free
mem	2,070,848	1,995,256	75,592
swap	2,097,144	112	2,097,032
total	4,167,992	1,995,368	2,172,624

You should configure your swap space to be at least twice the size of your physical memory.

4.4. **Disk Space**

After analyzing the disk space utilization of your SmartCenter we found that some of the partitions are at 74% capacity.

Solution: Consider enlarging your disk space when planning the migration.

Filesystem	1K-blocks	Used	Available	Use%	Mounted on
/dev/cciss/c0d0p7	602,340	422,792	148,952	74%	/
/dev/cciss/c0d0p1	150,128	9,991	132,386	8%	/boot
/dev/cciss/c0d0p2	1,546,064	728,160	739,368	50%	/opt
/dev/cciss/c0d0p6	1,546,064	593,852	873,676	41%	/sysimg
/dev/cciss/c0d0p3	5,320,205	630,280	4,689,925	12%	/var

4.5. **Support Contract Status**

Subscription is valid until January 2011

4.6. **Available HFA**

Your system runs R65 **HFA02** which is more than a year old, while **HFA70** for R65 is available for download on the Check Point user center. HFAs include performance, stability and security fixes and are very recommended.

