



Check Point[®]
SOFTWARE TECHNOLOGIES LTD.

CHECK POINT OPTIMIZATION REPORT

Prepared For: **ABC Inc**
Prepared by: **John Doe**
Check Point Software Technologies

3D
SECURITY



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

Table of Contents




EXECUTIVE SUMMARY	3
SYSTEM HEALTH	3
OBJECTS DATABASE	4
RULEBASE ANALYSIS	4
POLICY NAME: AN-SERVICE-INT	4
<i>Policy Optimization overview</i>	4
<i>RuleBase Risk Analysis and Best Practices</i>	4
IPS ANALYSIS	5
FINDINGS – POLICY OPTIMIZATION	6
POLICY OPTIMIZATION.....	6
RULE CONSOLIDATION.....	6
SECUREXL OPTIMIZATION	6
LOGGED RULES ANALYSIS*	7
<i>Most used logged rules</i>	7
LEAST USED LOGGED RULES	7
UNUSED LOGGED RULES	7
DISABLED RULES.....	8
FINDINGS – RULEBASE RISK ANALYSIS*	8
"ANY" USAGE IN RULES	8
REMIEDIATION	9
ABOUT CHECK POINT SOFTWARE TECHNOLOGIES	10

EXECUTIVE SUMMARY

The following document presents the result of a policy optimization project performed by Check Point.









The project examined the deployment of your Check Point solutions and identified opportunities to optimize your network security management system. Check Point analysts used a number of utilities that assess the usage of the security policy, its optimization potential and weaknesses. Combined with expert human analysis, the document identifies opportunities to improve overall management and gateway performance and security.

Each recommendation is rated as follow:

-  **Serious** – Needs immediate attention: 8 Items
-  **Attention** – Needs attention: 4 Items
-  **Good** - No need for any action: 21 Items

SYSTEM HEALTH

CMA Name: an-internal

	Status	Comments
Disk Usage		- /dev/sda7 - Warning
Memory Usage		- Free memory is below 20% - Error
License		
Contract		No contract coverage
Users		17 out of 17 local users expired
Anti-spoofing		12 interfaces need attention on anti-spoofing configuration
Global Properties		- No lockout policy - Drop Templates are disabled - TCP start timeout not default - TCP end timeout not default
Policies Assigned		All policies are assigned

OBJECTS DATABASE

Object database size affect policy installation time performance.

	Status	Count	Percent	remediation
Total Objects		5963	100%	N/A
Global Objects		1102	18.48%	N/A
Local Objects		4861	81.52%	N/A
Unused Objects		110	1.84%	Consider deleting these objects
Duplicate Objects		604	10.13%	Consider deleting copies
Nested Objects		7	0.12%	N/A

RULEBASE ANALYSIS

Policy Name: an-service-INT

Policy Optimization overview






General information about the current status of the active policy analyzed

	Status	Count	Percent	Remediation
Total rules		2238	100%	Size should be reduced
Optimization potential		261	11.66%	Policy size could be reduced by 261 rules
Rules disabling acceleration		22	4%	- 22 unique conditions - First disabled by rule #11


RuleBase Risk Analysis and Best Practices

Rulebase tend to grow with time and change requests, the table below summarizes the optimization potential our experts have found in your active policy.

	Status	Count	Percent	Remediation
Rules utilizing "Any"		56	2.5%	- ANY in Source: 20 - ANY in Destination: 14 - ANY in Service: 22
Disabled Rules		159	7.1%	
DNS Rules		58	2.59%	
Unnamed Rules		18	0.8%	Naming rules helps log analysis
Time Rules		13	0.58%	

Non Logging Rules		12	0.54%	
Stealth Rule				Not Found
Cleanup Rule				Found
Uncommented Rules		300	21%	Comment rules for better tracking and change management compliance
Section Title Usage		44		44 section tiles found

IPS ANALYSIS

	Status	Percent	Gateways Applied	Comments
Default_Protection		93.33	- au-office_INT - an-services_INT	- 68 Critical protections inactive - 2 Critical protections in detect only

FINDINGS – POLICY OPTIMIZATION

This is a sample only – actual finding presentation might be different or separate in the real report. Some of the features below are relevant for SmartOptimize Premium only.

Policy Optimization




Policy: ##Standard

Gateways policy is installed on: **CP-Perimeter**

Total number of rules that are applied to above gateways: 142

Total numbers of rules that will disabled SecureXL templates: 2

Rulebase Compliance

Stealth Rule	Cleanup Rule	SecureXL
		

Rule consolidation

The rules below were found to be in optimization potential, consolidating them will reduce the total number of rules complexity.

Rule # 422

ID	Source	Destination	Service	Track	Action	Comment
422	Any	Any	Any	Log	drop	Final drop

Rule #422 can be merged with:

ID	Source	Destination	Service	Track	Action	Comment
420	Any	Any	icmp-proto	Log	drop	

Rule # 352

ID	Source	Destination	Service	Track	Action	Comment
352	Any	srs-ili.test.com	https	Log	accept	Allow public access to https test

Rule #352 can be merged with:

ID	Source	Destination	Service	Track	Action	Comment
353	Any	bpo-ili.test.com	https	Log	accept	License servers

SecureXL optimization

Rule #1 will disable SecureXL template creation; Service ISAKMP has a source port defined

ID	Source	Destination	Service	Track	Action	Comment
1	Admin_Machines FW-DEV-Cluster DMZ_CMA	Admin_Machines FW-DEV-Cluster DMZ_CMA	http ftp SSH_22 ISAKMP	Log	accept	Allows Paris to communicate using HTTP/Telnet

Rule #23 will disable SecureXL template creation; Service dhcp_relay has a source port defined

ID	Source	Destination	Service	Track	Action	Comment
23	DHCP_Broadcast QIP02ROS QIP03ROS	DHCP_Broadcast QIP03ROS	dhcp_relay dhcp-req- localmodule dhcp-rep	Log	accept	Rule set up as part of DHCP broadcast testing

Logged Rules analysis*

* Available in SmartOptimize Premium only

Most used logged rules

Top most used rules should be placed at the top of the rulebase, based on your deployment and security architecture.

Policy: Standard

Rule #	connections	% of total connections
240	73,439	66.83%
179	16,933	15.41%
434	7,975	7.26%

Least used logged rules

Least used rules should be placed at the bottom of the rulebase, based on your deployment and security architecture.

Rule #	connections	% of total connections
8	968	0.97%
29	675	0.68%
34	142	0.14%

Unused logged rules

Unused logged rules represent rules that were not hit, based on the logs analysis and might be used in rare occasions. It's recommended to first disable the following rules and monitor whether they are still needed before deletion.

Rule #	55, 78, 113, 191, 250, 805
--------	----------------------------

Disabled Rules

The following rules are disabled; it's recommended you verify whether it's still needed, and delete it upon verification that the rules are redundant.

ID	Name	Source	Destination	Service	Track	Action	Comment
21		Machine_Testit Machine_Whatis	Google_Networks	https	Log	accept	Needed for blogger.com access

FINDINGS – RULEBASE RISK ANALYSIS*

* Available in SmartOptimize Premium only

The rulebase analysis also run through a series of tests where rules using "Any" in particular fields are tested and analyzed based on the log analysis. These rules pose potential security risk and it is our recommendation to avoid it when possible.

"Any" usage in rules

ANY in Source: 18

ANY in Destination: 7

ANY in Service: 43

Potential issue: 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: Standard

Rule: 61

ID	Name	Source	Destination	Service	Track	Action	Comment
61	Production Web Applications	Any	ilz-forums-LS ilz-getsecure-LS ilz-pricelist-LS ilz-usercenter-LS ilz-register-LS	http https	Log	accept	

Recommendation: The following list shows the result of our analysis of your logs, consider using this **sources** separately or in a network group instead of using "Any", like shows in the rule below:

ID	Name	Source	Destination	Service	Track	Action	Comment
61	Production Web Applications	157.35.22.12, 192.168.2.2, 135.15.1.1, 166.3.3.1, 190.168.2.33, 190.168.2.48	ilz-forums-LS ilz-getsecure-LS ilz-pricelist-LS ilz-usercenter-LS ilz-register-LS	http https	Log	accept	

REMEDIATION

The following table is the summary of this report, specifying the actual issues, risks associated and remediation potential as found in our analysis, it will explain the issue and then guide you to the relevant part of this report that explains our recommendation in detail.

Only issues marked as "Attention" or "Critical" are displayed below.

Policy Optimization	
Rulebase size	remediation
Rulebase size is the finite number of rules in an active policy, including active, unused, and disabled rules. Policy size is also a key factor in the policy installation time (compilation).	Check Point recommends having the rulebase size in the final number of a few hundreds top, it's clear that a smaller rulebase is not only easier to manage and administer, but also has less risk of potential security breaches or redundant rules. Please follow the steps below related to this section and reduce the size of your rulebase accordingly.
Unused logged rules	remediation
Unused rules are mostly leftovers from past change requests and change in administrators that didn't have the ability or knowledge to delete them. Those rules pose an unnecessary burden on the active policy in terms of administration and indirect impact on performance.	Check Point recommends placing unused rules in "monitor" status, by disabling them and setting an ultimatum to their deletion, then delete them after the monitoring period. Please see "Policy Optimization" section --> Unused logged rules.

Additional remediation items will appear here depending on the outcome of your analysis.

ABOUT CHECK POINT SOFTWARE TECHNOLOGIES

Check Point Software Technologies' (www.checkpoint.com) mission is to secure the Internet. Check Point was founded in 1993, and has since developed technologies to secure communications and transactions over the Internet by enterprises and consumers.

When the company was founded, risks and threats were limited and securing the Internet was relatively simple. A firewall and an antivirus solution generally provided adequate security for business transactions and communications over the Internet. Today, enterprises require many (in some cases 15 or more) point solutions to secure their information technology (IT) networks from the multitude of threats and potential attacks and are facing an increasingly complex IT security infrastructure.

Check Point's core competencies are developing security solutions to protect business and consumer transactions and communications over the Internet, and reducing the complexity in Internet security. We strive to solve the security maze by bringing "more, better and simpler" security solutions to our customers.

Check Point develops markets and supports a wide range of software, as well as combined hardware and software products and services for IT security. We offer our customers an extensive portfolio of network and gateway security solutions, data and endpoint security solutions and management solutions. Our solutions operate under a unified security architecture that enables end-to-end security with a single line of unified security gateways, and allow a single agent for all endpoint security that can be managed from a single unified management console. This unified management allows for ease of deployment and centralized control and is supported by, and reinforced with, real-time security updates.

Check Point was an industry pioneer with our FireWall-1 and our patented Stateful Inspection technology. Check Point has recently extended its IT security innovation with the development of our Software Blade architecture. The dynamic Software Blade architecture delivers secure, flexible and simple solutions that can be customized to meet the security needs of any organization or environment.

Our products and services are sold to enterprises, service providers, small and medium sized businesses and consumers. Our Open Platform for Security (OPSEC) framework allows customers to extend the capabilities of our products and services with third-party hardware and security software applications. Our products are sold, integrated and serviced by a network of partners worldwide. Check Point customers include tens of thousands of businesses and organizations of all sizes including all Fortune 100 companies. Check Point's award-winning ZoneAlarm solutions protect millions of consumers from hackers, spyware and identity theft.