CHECK POINT™

YOU DESERVE THE BEST SECURITY

CHECK POINT
PROFESSIONAL SERVICES
Consult • Design • Deploy • Operate • Optimize

CHECK POINT SMARTOPTIMIZE REPORT

Prepared for	By	Date
<Customer ACME>	<PS Consultant>	<Date>

Table of Contents

Check Point Professional Services

DMZ – Management Report

Executive Summary

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

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, gateway performance and security.

Each recommendation is rated as follow:

Serious: Needs immediate attention 8 Items

Attention: Needs attention 15 Items.

Good: No need for any action 23 Items.

System Health

Monitoring the system health of your Check Point solutions is critical to identify health issues before they affect system resources. The table below provides a summary on the system health of your management server.

This is Check Point Security Management Server R80.10 - Build 011 (No hotfixes)

	Status	Comments
Disk Usage		
Memory Usage		
License		
Contract		2 out of 4 contracts are expired.
Policies Assigned		3 out of 6 policies are not assigned.
Service Analysis		Some of the services are not using their default timeouts. For more details refer to System Report.

Objects Database

The objects database size can affect performance and policy installation time. The table below provides a summary of the network objects database.

	Status	Count	Percent	Remediation
Total Network Objects	✓	45786	100%	
Unused Network Objects	✓	4	0.01%	
Duplicate Network Objects	✗	6456	14.1%	Consider deleting copies.
Nested Network Objects	✓	395	0.86%	

Services Database

The services database size can affect performance and policy installation time. The table below provides a summary of the services objects database.

	Status	Count	Percent	Remediation
Total Services Objects	✓	1375	100%	
Unused Services Objects	⚠	46	3.35%	Consider deleting these objects.
Nested Services Objects	✓	7	0.51%	

Rulebase Analysis

Policy Optimization Overview
The tables below provides general information about the current status of the active policies analyzed.

RuleBase Risk Analysis and Best Practices
Rulebase tend to grow with time and change requests, the tables below summarize the optimization potential our experts have found in your active policies.

Policy: DMZ-VSX-policy

	Status	Count	Percent	Remediation
Total Rules	✓	77	100%	
Rules utilizing "Any"	✗	21	27.27%	- ANY in Source: 5 - ANY in Destination: 14 - ANY in Service: 2
Disabled Rules	⚠	3	3.9%	Check if rules are required.
Unnamed Rules	⚠	30	38.96%	Naming rules helps log analysis.
Times Rules	✓	0	0%	
Non Logging Rules	⚠	20	25.97%	Log rules for better rules tracking.

Stealth Rule	✗			Not Found
Cleanup Rule	✓			Found
Uncommented Rules	⚠	6	7.79%	Comment rules for better tracking and change management compliance.
Section Titles	✓	20		20 section titles found.
Optimization Potential	✓	1	1.35%	

Policy Hit-Count Overview

The tables below provides information about the misplaced rules in the active policies across all security layers.

	Rules Hit	Top Hit Rules	Misplaced Rules	Zero Hit Rules
Global Policy	72	6	5	12
Database Policy Layer	1	0	0	1
DMZ-VSX-policy Security	4	1	0	0

Policy: DMZ1-policy

	Status	Count	Percent	Remediation
Total Rules	✓	190	100%	
Rules utilizing "Any"	✗	39	20.53%	- ANY in Source: 13 - ANY in Destination: 21 - ANY in Service: 5
Disabled Rules	⚠	4	2.11%	Check if rules are required.
Unnamed Rules	⚠	123	64.74%	Naming rules helps log analysis.
Times Rules	✓	0	0%	
Non Logging Rules	⚠	23	12.11%	Log rules for better rules tracking.
Stealth Rule	✗			Not Found
Cleanup Rule	✓			Found
Uncommented Rules	⚠	3	1.58%	Comment rules for better tracking and change management compliance.
Section Titles	✓	49		49 section titles found.
Optimization Potential	✓	10	5.35%	

Policy Hit-Count Overview
The tables below provides information about the misplaced rules in the active policies across all security layers.

	Rules Hit	Top Hit Rules	Misplaced Rules	Zero Hit Rules
Global Policy	72	6	5	12
DMZ1-policy Security	118	10	4	12

Policy: DMZ2-policy

	Status	Count	Percent	Remediation
Total Rules	✓	123	100%	
Rules utilizing "Any"	✗	30	24.39%	- ANY in Source: 8 - ANY in Destination: 18 - ANY in Service: 4
Disabled Rules	⚠	21	17.07%	Check if rules are required.
Unnamed Rules	⚠	65	52.85%	Naming rules helps log analysis.
Times Rules	✓	0	0%	
Non Logging Rules	⚠	23	18.7%	Log rules for better rules tracking.
Stealth Rule	✗			Not Found
Cleanup Rule	✓			Found
Uncommented Rules	⚠	7	5.69%	Comment rules for better tracking and change management compliance.
Section Titles	✓	31		31 section titles found.
Optimization Potential	✓	2	1.65%	

	Rules Hit	Top Hit Rules	Misplaced Rules	Zero Hit Rules
Global Policy	72	6	5	12
DMZ22-policy Security	51	10	10	21

Consultant Comments

PLEASE UPDATE THE SECTION BELOW WITH RELEVANT COMMENTS AND FINDINGS
THANKS TO Jon P FOR THE TEMPLATE
This SmartOptimize service took an export of the XYZ Check Point management station and submitted it for review by Check Point Professional Services. This document is the result of that analysis and will help XYZ to provide maximum protection for their information assets, employees and Governance / Risk and Compliance (GRC) auditing.

The general feedback is that the Check Point configuration is adequate but improvements must be made to reach the standard of “best practice“.

The steps below and in the supporting documentation will help XYZ significantly. However, the fact that FILL IN AS REQUIRED.

The transformation could take several weeks of effort. Check Point Professional Services can support XYZ through this transition and ensure that the Check Point installed products are optimally utilized.

Remediation Recommendations

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.

System Health	
Contract	**Remediation**
Contracts complete licenses and are the support availability behind every product you own. These contract signify your ability to receive support, and are stored in encrypted text files on your management station. They might be required for certain maintenance and/or upgrade operations.	If your contracts files are not valid, expired or not installed, please follow the steps in section "Health check" to remediate the problem.
Users	**Remediation**
Local users are defined when internal authentication is used with remote VPN and other functionalities. These users are stored encrypted in fwauth.NDB file and are important to the proper usage of VPN in your system. Too many users can cause overhead, so redundant ones should be removed.	Please follow instructions related to users cleanup and or activities in the "health check section.
Anti-Spoofing	**Remediation**
"Spoofing" is when an attacker is masking his IP address to appear as if it's another, mostly from an internal/trusted network in order to bypass security devices. "Anti-Spoofing" is a security mechanism by Check Point (available on all GWs) that allows identifying such attempts easily based on the GW's topology.	Check Point recommends enabling "Anti-spoofing" by configuring the topology properly on all GWs using static routing configurations. Please refer to "SystemInfo" document to see a list of incompliant security GWs.
Global Properties	**Remediation**
Global Properties are set of rules and configurations that are valid throughout the system and configured centrally; these include some security features that therefore have affect system-wide. Accessing these properties are available from "Policy" --> "Global Properties".	Check Point recommends reviewing the items found in our analysis, as appearing in "SystemInfo" document.
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 hundred 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.

Rules Disabling Acceleration	Remediation
There are certain protocols and other rule properties that partially or fully disable the ability of the Security GW to use some of its acceleration technologies. Some of these disabled features might include you are not using the full extent of your appliance performance with relation to Session rate and packets per second.	Check Point recommends considering changing the order of these rules to accommodate better performance, rules disabling acceleration should be moved further down the rulebase (as long as they are not one of the top most rules). Follow the analysis provided by "SecureXLReport" .
Rules Disabling Acceleration	**Remediation**
In our experience FW administrators tend to add rules needed by business needs and in time pressure. These rules might actually be consolidated into existing rules, thus reducing the complexity of the rulebase and its efficiency. Less rules means more efficient and easier to administrate.	Check Point recommends consolidating similar rules to minimize complexity and size of the rulebase. In the "PolicyOptReport" document we have used our latest analysis tools to offer you the list of the rules we feel should be optimized. This will result is reduction of the total number of rules.

Basic Risk Analysis	
Rulebase Utilizing "Any"	**Remediation**
"Any" is an option that can be used in the rulebase as a generic option for source, destination or service. However, this is not a secure manner of usage in rules, as it might allow unauthorized access and or usage of services.	Check Point recommends minimizing the use of "Any" in rules, especially in rules that are allowing traffic to or from the WAN. Please refer to "RuleBaseReport" document for more details.
Disabled Rules	**Remediation**
Disabled rules are rules that are part of the management database, but do not transfer to the GW as part of its policy. These rules are probably not needed due to their expiration or irrelevancy over time.	Check Point recommends observing the Disabled rules and "marking" them for deletion. Delete the rules after you have certainty that they are not used. You can use the "unused logged rules" to verify that if these rules are also logged.
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 "RuleBaseReport" document.

Disclaimer

The Customer hereby attests and acknowledges that the Check Point Professional Services Engineer has completed the project work described above. This work meets the requirements specified by the Customer and has been completed to the satisfaction of the Customer.

By:	By: <NAME>
Authorized Customer Representative	Check Point Professional Services Representative
Date:	Date: <DATE>

Post Project Contact Information

Technical Issues
Check Point Software offers a wide variety of additional Assistance methods for their customers. Check Point Software offers direct customer support though our Worldwide Technical Assistance Centers for customers who purchase a support contract. Customers may also purchase follow-up telephone support assistance from Professional Services. Alternatively, a customer may work with a local Check Point reseller for support.

Check Point Professional Services
We offer follow-up telephone support at the rate of $800 per ½ day. Please contact us for this or any other future Professional Services project needs.

E-mail: ps@checkpoint.com
Phone: +972-3-7534796

Check Point Technical Support
Our Worldwide Technical Assistance Centers are available to assist you 24x7.

Americas: 972-444-6600
International (Non-US): +972-3-6115100
E-mail: support@ts.checkpoint.com
Web: http://support.checkpoint.com
Please provide your organization's support number when contacting Technical Services.

Check Point Sales
To find a Check Point Reseller:
Phone: 1-800-429-4391
E-mail: sales@checkpoint.com
Web: http://www.checkpoint.com/sales/index.html