

SmartUse

Optimize your Check Point deployment

YOUR CHALLENGE

Your organization's network is a robust and sophisticated infrastructure, but it is also constantly evolving. Elements are continually added, deleted, moved, modified, and updated. These changes in the network environment are reflected in your security arsenal. As your network deployment changes, so do the corresponding security policies and configurations. Now here comes the challenge: With a constantly changing network and security environment, how do you keep your security components optimized and working in harmony? In other words, is your security infrastructure optimized for defense, performance, and stability? Or has the constantly changing environment created weak links in your security arsenal or prevented your security from operating at optimum performance?

OUR SOLUTION

Check Point SmartUse is a service that performs a deep analysis of your Check Point implementation. Under a strict confidentiality agreement, we will perform a thorough analysis of configuration and log data from your Management Server. The result of this analysis is a detailed report that summarizes our findings and provides you with concrete and actionable recommendations on how to optimize and strengthen the security and performance of your Check Point solutions. A Check Point technical expert will review all findings and recommendations with you.

WHAT IS SMARTUSE?

Check Point SmartUse is a service that performs a deep analysis of your Check Point implementation. The result is a detailed analysis, and actionable recommendations for optimizing and strengthening your security deployment.

HOW IT WORKS

- Order one report or a yearly subscription
- Send us your configuration data and log files for at least one typical 24-hour work day
- Our experts will analyze the data and create a report with detailed findings and recommendations
- Each report is created and thoroughly reviewed by Check Point security experts
- You will receive the report and review it over the phone with the security expert who prepared it

“The report was clear and precise...remarks were to the point.”

Customer, SmartUse Service

EXTENSIVE COVERAGE

Table of contents of a report

1	Executive Summary.....	3
2	Security and Stability Improvements.....	5
2.1	✘ SmartDefense Protections.....	5
2.2	⚠ Rule Base Improvements.....	8
2.3	✔ Configuration Changes since Last Review.....	10
2.4	⚠ Database Integrity.....	11
3	Rule Base Performance Improvements.....	12
3.1	⚠ Most Active Rules.....	12
3.2	⚠ Least Active Rules.....	13
3.3	⚠ Unused Objects.....	13
3.4	⚠ Duplicated Objects.....	14
3.5	⚠ Rule Base Size Optimization.....	14
4	Additional Recommendations.....	15
4.1	⚠ Administrator and User Management.....	15
4.2	✘ System Related Recommendations.....	16
4.3	✔ Support Contract Status.....	16
4.4	✘ Version Management.....	16

TRUST THE EXPERTS

No one is more qualified to help you optimize your Check Point security arsenal than the experts who created it. We will leverage our extensive knowledge and expertise to provide you with concrete and relevant recommendations for your deployment.

CONTENTS OF THE SMARTUSE REPORT

The SmartUse Report contains detailed findings and recommendations about many aspects of your Check Point deployment, including:

- Security and stability improvements
 - SmartDefense™ protection findings and recommendations
 - Rule-based and security policy consistency recommendations
 - Database integrity recommendations for improved stability and security
- Rule-based performance improvements
 - Analysis of most- and least-used rules and recommendations for optimizing rule sequence to enhance performance
 - Identification of, and recommendations for, redundant and unused rule-based objects
- Administrator management improvements
 - Analysis of administrator
 - Recommendations dealing with security aspects of user management
- System-related recommendations
 - Analysis and recommendations dealing with global system settings, version management, hot-fix status, etc.
- Many more findings and practical recommendations

To learn more, or to download and evaluate a sample SmartUse Report, please contact your Check Point reseller or visit www.checkpoint.com/services.

SAMPLE SMARTUSE REPORT CONTENT

Security weaknesses identified and corrective actions suggested

2.2.2 Rulebase Security Improvements

You network contains several rules that allow connections into the internal network from outside the organization. Such rules can compromise your overall security and enable direct connection from the web.

We recommend that you modify your policy to enhance security.

The following three rules (28, 49, and 51) pose a security risk.

Rule 28: SRC Any; DEST YoesllS; VPN Any; SVC http; ACTION Accept

Solution: Since a hacker can get a remote shell on the server and access the entire network the HTTP server should be in DMZ.

ID	NAME	SOURCE	DESTINATION	VPN	SERVICE	ACTION	TRACK	INSTALL ON	TIME
28		Any	YoesllS	Any Traffic	HTTP	Accept	Log	Policy Targets	Any

Potential stability and management traps identified and addressed

2.4 Database Integrity

The following recommendations are based on a database integrity test. We recommend that you deal with these issues as soon as possible since they can cause problems during policy management and upgrades.

Problem: *gftp service: Accept replies from any port.*

Solution: Verify that *Accept replies from any port* is not selected, since it allows Stateful UDP replies from any port. Go to **Service Properties > Advanced > Accept replies from any port**. This change should not affect connectivity.

Extensive performance-related analysis and recommendations provided

3.1 Most Active Rules

The following are the most active rules in your "corporate-new-simplified" security policy. To improve performance, consider moving these rules (214, 218, 153, 190 and 39) to the beginning of the rule base.

Rule Number	Number of Connections	% of Total Connections
214	401,854	49.36%
Implied	113,106	13.89%
218	82,258	10.10%
153	78,328	9.62%
190	34,993	4.30%
39	29,603	3.64%

CONTACT CHECK POINT

Worldwide Headquarters

5 Ha'Solelim Street, Tel Aviv 67897, Israel | Tel: 972-3-753-4555 | Fax: 972-3-575-9256 | Email: info@checkpoint.com

U.S. Headquarters

800 Bridge Parkway, Redwood City, CA 94065 | Tel: 800-429-4391; 650-628-2000 | Fax: 650-654-4233 | www.checkpoint.com