NETBRIGHT
ENTERPRISE IT SOLUTIONS

Firewall Rule Optimizer

เครื่องมือตรวจสอบและปรับแต่งกฎไฟร์วอลล์

User Manual · คู่มือการใช้งาน

1. Introduction 1. บทนำ

This manual explains how to use the Firewall Rule Optimizer to analyze and improve firewall policies for Palo Alto, Fortinet, Cisco, and Check Point. The tool runs entirely in your web browser; no data is sent to any server.

คู่มือนี้อธิบายวิธีใช้ Firewall Rule Optimizer เพื่อวิเคราะห์และปรับปรุงนโยบายไฟร์วอลล์สำหรับ Palo Alto, Fortinet, Cisco และ Check Point เครื่องมือนี้ทำงานภายในเบราว์เซอร์ทั้งหมด ไม่มีการส่งข้อมูลไปยังเซิร์ฟเวอร์

2. Getting Started 2. เริ่มต้นใช้งาน

1. Open https://firewall-optimizer.vercel.app in a modern browser (Chrome, Edge, Firefox, or Safari).
   เปิด https://firewall-optimizer.vercel.app ในเบราว์เซอร์รุ่นใหม่ (Chrome, Edge, Firefox หรือ Safari)
2. The screen has two panels: Configuration Input on the left and Results on the right. Findings and the parsed rule table appear below after analysis.
   หน้าจอมีสองส่วน: ช่องนำเข้าคอนฟิก (ซ้าย) และผลลัพธ์ (ขวา) ส่วนรายการปัญหาและตารางกฎจะปรากฏด้านล่างหลังการวิเคราะห์
3. Use the theme button (top-right) to switch between dark and light modes.
   ใช้ปุ่มธีม (มุมขวาบน) เพื่อสลับระหว่างโหมดมืดและสว่าง

3. Analyzing a Configuration 3. การวิเคราะห์คอนฟิก

1. Select the vendor with the format toggle (Auto, Palo Alto, Fortinet, Cisco, Check Point). "Auto" detects the format automatically.
   เลือกผู้ผลิตจากปุ่มเลือกรูปแบบ (Auto, Palo Alto, Fortinet, Cisco, Check Point) โหมด "Auto" จะตรวจจับรูปแบบให้อัตโนมัติ
2. Paste your configuration into the input box, or click Upload (or drag a file in). Click "Load sample" to try a built-in example.
   วางคอนฟิกลงในช่องนำเข้า หรือคลิก Upload (หรือลากไฟล์มาวาง) คลิก "Load sample" เพื่อทดลองด้วยตัวอย่างในระบบ
3. (Optional) Expand "Add hit-count data" and paste rule hit counts to enable unused-rule detection and traffic-based ordering.
   (ไม่บังคับ) ขยายส่วน "Add hit-count data" แล้ววางข้อมูลจำนวนครั้งที่กฎถูกใช้ เพื่อเปิดการตรวจกฎที่ไม่ถูกใช้และการจัดลำดับตามทราฟฟิก
4. Click the Analyze button (or press Ctrl/Cmd+Enter).
   คลิกปุ่ม Analyze (หรือกด Ctrl/Cmd+Enter)
5. Review the Security Score, the Findings tabs, and the parsed rule table.
   ตรวจสอบคะแนนความปลอดภัย แท็บรายการปัญหา และตารางกฎที่อ่านได้

4. Understanding the Results 4. การตีความผลลัพธ์

The Security Score (0–100) and grade summarize overall policy hygiene. Findings are grouped into tabs:

คะแนนความปลอดภัย (0–100) และเกรด สรุปสุขอนามัยของนโยบายโดยรวม รายการปัญหาถูกแบ่งเป็นแท็บดังนี้:

Finding tab	ความหมาย
Exposure — overly-permissive and any-any allow rules	Exposure — กฎที่อนุญาตกว้างเกินไปและกฎ any-any
Compliance — pass/fail against CIS and PCI-DSS controls	Compliance — ผ่าน/ไม่ผ่าน ตามมาตรฐาน CIS และ PCI-DSS
Unused — rules with zero hits (needs hit-count data)	Unused — กฎที่ไม่ถูกใช้ (ต้องมีข้อมูล hit-count)
Shadowed — rules hidden by an earlier broader rule	Shadowed — กฎที่ถูกบดบังโดยกฎก่อนหน้าที่กว้างกว่า
Redundant — exact duplicate rules	Redundant — กฎที่ซ้ำกันทุกประการ
Mergeable — rules that can be combined into one	Mergeable — กฎที่รวมเป็นกฎเดียวได้
Ordering — rules that could be reordered for speed	Ordering — กฎที่ควรจัดลำดับใหม่เพื่อความเร็ว
Good — healthy practices detected	Good — แนวปฏิบัติที่ดีที่ตรวจพบ

Each finding shows a severity (high / medium / low), an explanation, and a suggested fix. Severity colors: red = high, amber = medium, cyan = low/info, green = good.

แต่ละรายการแสดงระดับความรุนแรง (สูง / กลาง / ต่ำ) คำอธิบาย และแนวทางแก้ไข สีระดับความรุนแรง: แดง = สูง, เหลือง = กลาง, ฟ้า = ต่ำ/ข้อมูล, เขียว = ดี

5. Hit-Count Data (Optional) 5. ข้อมูล Hit-Count (ไม่บังคับ)

Provide rule usage counts to find rules that never match traffic and to order rules by real usage. Paste one rule per line as "name, count" or "name count".

ใส่จำนวนครั้งที่กฎถูกใช้ เพื่อค้นหากฎที่ไม่เคยตรงกับทราฟฟิก และจัดลำดับกฎตามการใช้งานจริง วางบรรทัดละหนึ่งกฎในรูปแบบ "ชื่อ, จำนวน" หรือ "ชื่อ จำนวน"

Vendor	Command to obtain hit counts
Palo Alto	show rulebase security rules hit-count
Fortinet	diagnose firewall iprope show <policyid> / policy hit count in GUI
Cisco ASA	show access-list <name> (per-line hitcnt)
Check Point	Rulebase hit-count column in SmartConsole

6. Generating an Optimized Config 6. การสร้างคอนฟิกที่ปรับปรุงแล้ว

1. After analysis, open the "Optimized configuration" panel.
   หลังการวิเคราะห์ ให้เปิดแผง "Optimized configuration"
2. The tool removes redundant and dead (shadowed) rules and, where the vendor supports it, applies safe merges.
   เครื่องมือจะลบกฎซ้ำซ้อนและกฎที่ตายแล้ว (ถูกบดบัง) และรวมกฎที่ปลอดภัยเมื่อผู้ผลิตรองรับ
3. Use Copy or Download to take the result. For Cisco, merges are listed but not auto-applied because they require object-groups.
   ใช้ Copy หรือ Download เพื่อนำผลลัพธ์ไปใช้ สำหรับ Cisco การรวมกฎจะแสดงไว้แต่ไม่ทำให้อัตโนมัติ เนื่องจากต้องใช้ object-group

4. Always review the generated config in a test/change window before applying to production.
ควรตรวจทานคอนฟิกที่สร้างขึ้นในช่วงทดสอบ/หน้าต่างเปลี่ยนแปลงทุกครั้งก่อนใช้งานจริง

7. Exporting a Report 7. การส่งออกรายงาน

Click "Export report" in the Findings panel to download a text report containing the score, counts, and every finding with its suggested fix — suitable for audit records.

คลิก "Export report" ในแผงรายการปัญหา เพื่อดาวน์โหลดรายงานข้อความที่มีคะแนน จำนวนต่าง ๆ และทุกรายการปัญหาพร้อมแนวทางแก้ไข เหมาะสำหรับเก็บเป็นหลักฐานการตรวจสอบ

8. Frequently Asked Questions 8. คำถามที่พบบ่อย

Is my firewall configuration uploaded anywhere? / คอนฟิกของฉันถูกอัปโหลดที่ใดหรือไม่?

No. All parsing and analysis happen in your browser. Nothing is sent to a server.
ไม่ การอ่านและวิเคราะห์ทั้งหมดเกิดขึ้นในเบราว์เซอร์ของคุณ ไม่มีการส่งไปยังเซิร์ฟเวอร์

Can I trust the optimized config blindly? / เชื่อถือคอนฟิกที่ปรับปรุงแล้วได้ทันทีหรือไม่?

Treat it as a reviewed suggestion. Validate in a change window; the analysis is heuristic.
ควรถือเป็นข้อเสนอแนะที่ต้องตรวจทาน ทดสอบในหน้าต่างเปลี่ยนแปลงก่อน เนื่องจากเป็นการวิเคราะห์เชิงประมาณการณ์

Are the CIS/PCI labels an official audit? / ป้าย CIS/PCI ถือเป็นการตรวจประเมินอย่างเป็นทางการหรือไม่?

No. They point you to the relevant control to guide a review; a formal assessment still needs a qualified assessor.
ไม่ เป็นเพียงการชี้ไปยังมาตรฐานที่เกี่ยวข้องเพื่อช่วยการตรวจสอบ การประเมินอย่างเป็นทางการยังต้องใช้ผู้ประเมินที่มีคุณสมบัติ

Nothing parsed — what now? / อ่านคอนฟิกไม่ได้ ควรทำอย่างไร?

Check the format toggle matches your vendor, or set it manually instead of Auto.
ตรวจสอบว่าปุ่มเลือกรูปแบบตรงกับผู้ผลิต หรือเลือกด้วยตนเองแทนโหมด Auto

> **Disclaimer: The analysis is heuristic and provided as guidance. Always review suggestions and test changes before applying them to production systems.**
> ข้อจำกัดความรับผิด: การวิเคราะห์เป็นเชิงประมาณการณ์เพื่อเป็นแนวทางเท่านั้น ควรตรวจทานข้อเสนอแนะและทดสอบการเปลี่ยนแปลงก่อนนำไปใช้กับระบบจริงเสมอ