AI-Policy Optimizer

for FortiGate Firewall

Automated Policy Analysis · Severity Classification · Change Review

Table of Contents

APO Tool — Agenda

Background & Challenges

Why APO? — Limitations of Manual Firewall Policy Management

Accumulated Unreviewed Policies

Hundreds to thousands of firewall rules maintained for years without proper review, creating security blind spots.

Limits of Manual Review

Checking policies one by one in Excel → excessive time consumption and inconsistent evaluation criteria per analyst.

No Visibility into Policy Usage

Lack of Hit Count and Last Used data makes it impossible to identify which policies are actually in use.

Difficult Change History Tracking

No standardized tool to compare FortiGate configurations before and after changes.

Current Workflow

Security Audit Response — Firewall Policy Optimization Process

Current Process Flow

~1 Week Per Device

01 — Security Team
Request policy optimization result list

02 — Infra Team
Extract all policies
Filter / Manual work

03 — Security Review
Apply additional criteria
Manual Excel work

04 — Infra Review
Review results &
Coordinate feedback

05 — Firewall Work
Execute changes on the firewall

Key Pain Points

① Repeated Round-Trip Communication

Security ↔ Infra Team: files exchanged at least 3 times per review cycle

② Inconsistent Manual Evaluation

Excel-based work leads to different results depending on the analyst

③ Enormous Time Cost

~1 week for Infra Team per device, plus additional Security Team verification

Both teams process the same data independently — APO consolidates this into a single automated workflow.

Improved Workflow with APO

Streamlined Security Audit Response — After APO Adoption

New Process Flow

From 5 Steps → 3 Steps

01

Infra Team

Provide Config & CSV files to Security

02

Security Team

Run APO · Extract result list · Send to Infra

03

Infra Team

Execute firewall changes from list

Infra Team Tasks

- Export FortiGate Config file (.conf/.txt)
- Export GUI Policy CSV (Hit Count, Last Used, Status)
- Share both files with Security Team

Security Team Tasks

- Run APO tool with provided files
- Extract deletion/disable/risky service target list
- Export Excel → forward to Infra Team

Infra Team Tasks

- Review APO-generated target list
- Execute firewall policy changes
- No negotiation round-trips required

Original 5-step process (3+ round-trips between teams) → Reduced to 3 steps with APO — results generated in a single pass.

Before vs. After APO

Manual Workflow vs. APO Automated Workflow

✕ Before APO (Current)

Work Time
~1 week per device

Workflow
Manual Excel / Email back-and-forth

Criteria
Varies by analyst / Inconsistent results

Audit Report
Custom format / Manual effort required

VS

✓ After APO

Work Time
Automated analysis within minutes

Workflow
Auto-generated after Config file upload

Criteria
Unified 7-level Severity standard

Audit Report
One-click Excel report auto-generated

APO eliminates repetitive manual work for both teams — delivering consistent, reliable results in a fraction of the time.

APO Solution Overview

Upload FortiGate Config + GUI Policy CSV → Automatic Analysis · Classification · Comparison

Policy Analysis

- Policy parsing & statistics
- Unused / temporary policy filtering
- AI-assisted analysis support

Config Change Review

- Before/After comparison
- Added · Removed · Changed policies
- Object change detection

Severity Classification

- 7-level automated severity scoring
- Recommended remediation actions
- Excel export

Single EXE (~35MB)

No Installation

Fully Offline

FortiOS 6.4~7.4

Windows 10/11 x64

Feature 01 — Policy Analysis

Policy Status Overview · Filtering

Input Files

- FortiGate Config file (.conf / .txt)
- GUI Policy CSV — incl. Hit Count · Last Used · Status
- Proxy Policy CSV (optional)

Config Summary

- Firewall policy count / Address objects / Service objects
- Interfaces · Schedules · Service groups
- Parsed result JSON download

Policy Table Filters

- Search by Policy Name / Src / Dst / Service
- Filter by Status (Enabled / Disabled)
- No HitCount / Expired Schedule / Risky Service filter
- No ITS Request — No Name / No RITM separation

Feature 02 — Configuration Change Review

Before / After Comparison · Change Detection

Upload two Config files (before and after) to automatically detect all changes.

Policy Changes

Added / Removed / Changed policy list
Policy ID · Name · Before/After detail comparison

Object Changes

Addresses · Address Groups · Services · Service Groups
System interface add/delete detection

Other Sections

Routing · VPN · Other FortiGate config sections
Name-based add/remove/change display

※ Schedule · Hit Count · Status (enabled/disabled) changes are excluded from comparison — operational noise filtering.

Feature 03 — Severity Classification

7-Level Automated Severity Scoring · Recommended Actions

APO analyzes FortiGate policies and automatically classifies security risk into 7 levels with recommended actions.

Lv.	Severity	Action	Condition
1	Critical	Disable Immediately	Risky services (FTP · TELNET, etc.)
2	High	Delete	Disabled policy / Expired schedule / Hit=0 old policy
3	Medium	Review Required	Any/All + Active (Server-User) / Temporary rule
4	Medium	Review Required	Any/All + Active (Server-Server)
5	Low	Submit ITS Ticket	Service ALL active S-U / VDI object / New S-U
6	Low	Submit ITS Ticket	Service ALL active S-S / AD · DNS / Infra · MGMT
7	None	Keep	Deny policy / ICMP Only / Valid ITS / Admin policy

Classification Logic (1/2)

Severity Engine — Priority Evaluation Order

Conditions are evaluated top-down. The first matching condition determines the final severity level.

Priority	Condition	Result	Description
① Override	severity_overrides object match	Assigned	VDI_135 → 5, individual overrides
② Deny	Action = deny / empty	7 (None)	Deny policies excluded from classification
③ ICMP	Service = ICMP Only	7 (None)	ICMP-only policies kept as-is
④ Valid ITS	RITM present + Schedule valid	7 (None)	Officially registered current policy
⑤ Any+ctrl	Src/Dst/Svc Any·All + 'controlled' keyword	7 (None)	Intentional broad-allow policy
⑥ Admin	ADMIN / MGMT object included	7 (None)	Admin policy retained
⑦ Risky Services	FTP · TELNET · TFTP · RLOGIN · RSH	1 or 3	Risky services / Mixed+active → 3

Classification Logic (2/2)

Severity Engine — Src/Dst Any · Service ALL · Temporary Rules

Condition	Traffic Type	Hit/Last Used	Result
Src/Dst Any + Svc Any (Full Allow)	All	Any	1 (Critical)
Src/Dst Any·All	Server-User	Active (≤1 yr)	3 (Medium)
Src/Dst Any·All	Server-Server	Active (≤1 yr)	4 (Medium)
Src/Dst Any·All + AD/DNS Services	—	—	6 (Low)
Src/Dst Any·All + Unused/Long-idle	—	Hit=0 or >1 yr	1 (Critical)
Service ALL only	Server-User	Active (≤1 yr)	5 (Low)
Service ALL only	Server-Server	Active (≤1 yr)	4 (Medium)
Temp keyword + No RITM	—	Hit>0 + >2 yrs	2 (High)
Temp keyword + No RITM	Server-User	Hit>0 + 1~2 yrs	3 (Medium)
Temp keyword + No RITM	Server-Server	Hit>0 + Recent	5~6 (Low)
Disabled Policy	—	Status=Disabled	2 (High)
Expired Schedule	—	Current month basis	2 (High)

Temporary keywords: 임시, Temp, temp, test, 테스트, 작업, migration, backup, old, BOSK, 이관

Traffic Type Classification

Server-User / Server-Server — Automatic Traffic Type Detection

Register User IP ranges in the IP Range Settings to enable automatic traffic type detection.

Server - User

Source or destination falls within the User IP range
→ User access policy (stricter criteria applied)

Server - Server

Both source and destination are within server IP ranges
→ Server-to-server policy (relatively relaxed criteria)

Unknown

User IP range not configured
→ Classified as Severity 0, prompts configuration

※ IP Range Settings location: Top menu → IP Range Settings
e.g. 10.0.0.0/8, 192.168.1.0/24 — enter your user IP ranges directly

Demo Flow

Step-by-Step Usage Guide

STEP 1

Run APO.exe (As Administrator)

Double-click after download
→ Browser auto-opens (localhost:5000)

STEP 2

Upload Config File

Click Config File button
→ Select .conf file
→ Config Summary displayed

STEP 3

Upload Policy CSV

Upload FW Policy CSV
→ Merges Hit Count Last Used · Status

STEP 4

Set User IP Range

IP Range Settings (top)
→ Enter user subnets
(enables S-U / S-S scoring)

STEP 5

Run Severity Scoring

Severity Results tab
→ Click Classify
→ 7-level results displayed

STEP 6

Export to Excel

Click Export Workbook
→ Results + detailed conditions downloaded

Expected Benefits & Licensing

Business Impact · Pricing

Faster Review

Days → Hours
Immediate priority identification via auto-scoring

Consistent Standards

Analyst-independent results
Same criteria applied every time

Reduced Security Risk

Critical policies identified instantly
Remediation actions auto-generated

Audit-Ready Reporting

Excel report auto-generated
Change history comparison recorded

License Information

Free Features	Policy browsing · Filtering · Config Diff · Severity view
Export Feature	Excel export — License key required
Purchase Method	Run APO → Click Export → Click 'Buy' button
Price & Purchase	https://choiceguidelab.com/apo-tool-ai-policy-optimizer/
License Type	One-time purchase, lifetime license · Offline validation · Instant email delivery

Export & License Purchase Guide

Download Result Report · How to Purchase

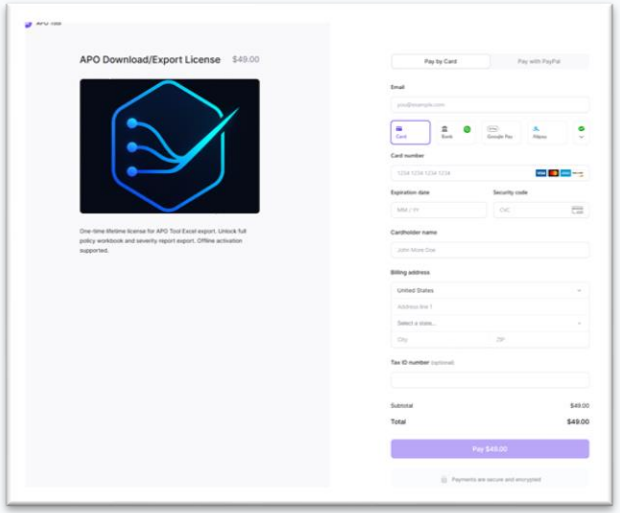
How to Export Result Report & Purchase License

① Click Download / Export button (internet required)

② License key entry popup appears

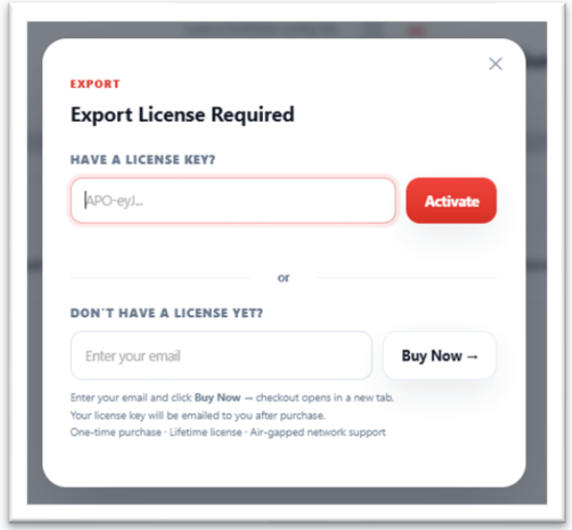
③ Enter your email address to receive the license key

④ Complete purchase on Lemon Squeezy payment site



⑤ License key sent immediately to your email

⑥ Copy key from email → click Activate button in APO



APO Tool Download

choiceguidelab.com — Free Download · Ready to Use Immediately

Visit the Website

Go to https://choiceguidelab.com/

Click APO Tool Category

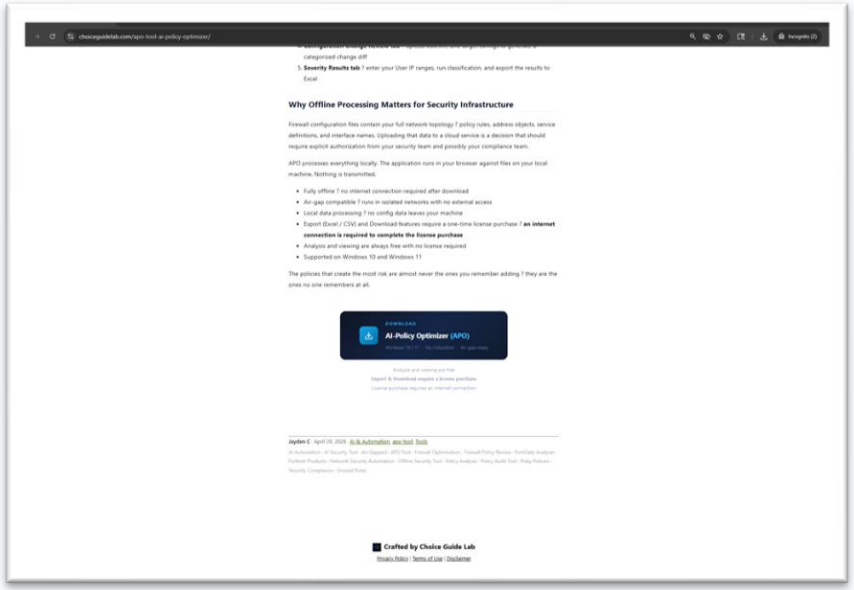
Select APO Tool category from the top menu

Open the Blog Post

Click the AI-Policy Optimizer (APO) blog post

Click Download Button

Click Tool Download button at the bottom of the post → Save APO.exe



https://choiceguidelab.com/apo-tool-ai-policy-optimizer/

Thank You

AI-Policy Optimizer for FortiGate

choiceguidelab.com/apo-tool-ai-policy-optimizer/