Adding Best Practices to Palo Alto Networks Next Gen Firewall

There are multiple tools for best practices on NGFW. Palo Alto Networks provides Best Practice Assessment for periodic security posture analysis and Expedition for feedback on optimizing policy. For health and stability, Indeni validates best practice and detects outage risks. To get started, consider the Indeni Best Practice Assessment guided trial, try the software yourself, or request a demo.

	Expedition	BPA	Indeni
Form factor	Downloadable VM or installation script to deploy on Ubuntu VM	Web app	Downloadable VM
Intended use	Policy migration, optimization, and suggestions based on traffic logs	Periodic assessment to improve security coverage per NGFW	Operational validation of stability and compliance across all NGFWs
Paradigm	Manual upload to local VM or cloud	Manual upload to cloud	NGFWs connected to on-prem VM
Frequency	Periodic	On demand	Continually
Input	Legacy firewall policy and/or Palo Alto Networks configuration and logs	TS TGZ file, manual mapping of interfaces, zones	Username, password IP for NGFW, connects to XML-API and SSH
Output	Palo Alto Networks NGFW policy (xml/set) and Ansible scripts	Multi-page heatmap, report, and recommended settings per finding	Individual notifications of current issues per NGFW, plus fix for each
Next step	Evaluate policy for suitability in environment	Identify and prioritize, implement, and repeat	Fix issues, prioritized in order of severity rating
Main users	Security engineering / architecture	Security audit	Operations
Main benefits	Accelerated deployment of NGFW from migrated policy, enriched with best practices, iron-skillets, and policy suggestions to reduce attack surface	Assessment of security posture, improvement recommendations, and historical overview to track progress	Real time detection and how-to-fix for issues that could lead to outages, plus best practice enforcement