Best Practice Assessment (BPA)

99% of firewall breaches through 2023 will be due to firewall misconfigurations, not firewall flaws, according to Gartner research.[1] Companies typically implement basic capabilities and postpone setting up many features that maximize protection.

Most organizations don't fully implement the capabilities of their Next-Generation Firewalls, leading to gaps in security. Use our free tool to quickly identify the most critical security controls for your organization to focus on. Confidently measure, track, and improve your security policy adoption.

Benefits of a Best Practice Assessment

- A quick and easy assessment that provides a barometer of your security implementation.
- Understand how to better protect your network by looking deep into your security policy adoption.
- Improve your security team's efficiency by following easy-to-action recommendations.

Why Run a Best Practice Assessment?

Adopting the built-in features of our Next-Generation Firewalls reduces network security risks. The Best Practice Assessment identifies opportunities for remediation, enabling you to:

- **Reduce re-work and change requests due to misconfigurations.** Ensure you're on top of your configurations and avoid receiving urgent calls about misconfigurations at the eleventh hour. Build confidence in your controls through visibility.
- **Quickly understand where to focus your security team's efforts.** Regular BPA scans can help your network administrative team prioritize tasks to address deficiencies.

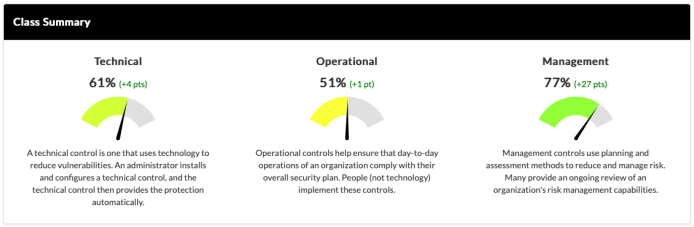
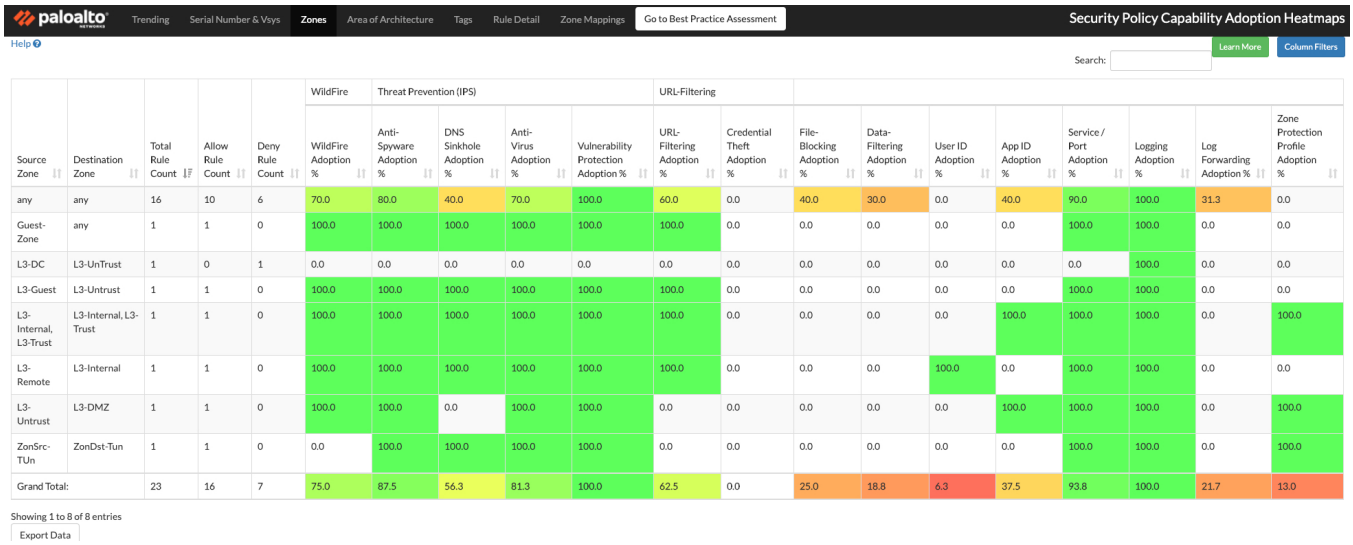


Figure 1: Best Practice Assessment (Class Summary)

- **See a best practice roadmap and track your progress.** Receive custom recommendations for critical policy configurations to address and measure the progress of your best practice implementation.



Source Zone	Destination Zone	Total Rule Count	Allow Rule Count	Deny Rule Count	WildFire: WildFire Adoption %	Threat Prevention (IPS): Anti-Spyware Adoption %	Threat Prevention (IPS): DNS Sinkhole Adoption %	Threat Prevention (IPS): Anti-Virus Adoption %	Threat Prevention (IPS): Vulnerability Protection Adoption %	URL-Filtering: URL-Filtering Adoption %	URL-Filtering: Credential Theft Adoption %	File-Blocking Adoption %	Data-Filtering Adoption %	User ID Adoption %	App ID Adoption %	Service / Port Adoption %	Logging Adoption %	Log Forwarding Adoption %	Zone Protection Profile Adoption %
any	any	16	10	6	70.0	80.0	40.0	70.0	100.0	60.0	0.0	40.0	30.0	0.0	40.0	90.0	100.0	31.3	0.0
Guest-Zone	any	1	1	0	100.0	100.0	100.0	100.0	100.0	100.0	0.0	0.0	0.0	0.0	0.0	100.0	100.0	0.0	0.0
L3-DC	L3-UnTrust	1	0	1	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	100.0	0.0	0.0
L3-Guest	L3-Untrust	1	1	0	100.0	100.0	100.0	100.0	100.0	100.0	0.0	0.0	0.0	0.0	0.0	100.0	100.0	0.0	0.0
L3-Internal, L3-Trust	L3-Internal, L3-Trust	1	1	0	100.0	100.0	100.0	100.0	100.0	100.0	0.0	0.0	0.0	0.0	100.0	100.0	100.0	0.0	100.0
L3-Remote	L3-Internal	1	1	0	100.0	100.0	100.0	100.0	100.0	100.0	0.0	0.0	0.0	100.0	0.0	100.0	100.0	0.0	0.0
L3-Untrust	L3-DMZ	1	1	0	100.0	100.0	0.0	100.0	100.0	0.0	0.0	0.0	0.0	0.0	100.0	100.0	100.0	0.0	100.0
ZonSrc-TUn	ZonDst-Tun	1	1	0	0.0	100.0	100.0	100.0	100.0	0.0	0.0	0.0	0.0	0.0	0.0	100.0	100.0	0.0	100.0
Grand Total:		23	16	7	75.0	87.5	56.3	81.3	100.0	62.5	0.0	25.0	18.8	6.3	37.5	93.8	100.0	21.7	13.0

Figure 2: Security Policy Capability Adoption Heatmap

1. Kaur, Rajpreet, Hils, Adam, and Watts, John, "Technology Insight for Network Security Policy Management," Gartner, Inc., February 21, 2019, https://www.gartner.com/en/documents/3902564/technology-insight-for-network-security-policy-managemen.

The BPA consists of three parts: the assessment itself, a Security Policy Capability Adoption Heatmap, and an executive summary.

The Best Practice Assessment is a focused evaluation of your adoption of security configuration best practices for Next-Generation Firewalls or Panorama™ network security management, grouped by policies, objects, networks, and devices.

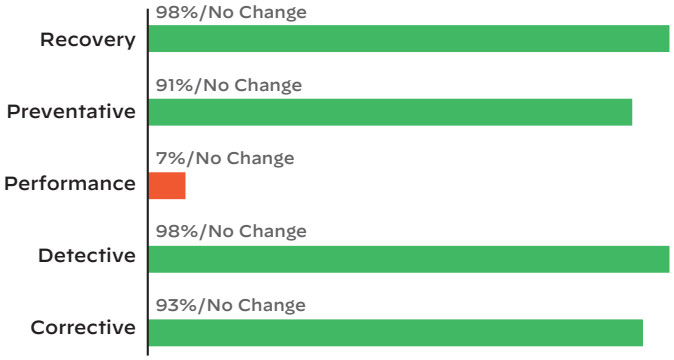


Figure 3: BPA Executive Summary

The Security Policy Capability Adoption Heatmap shows gaps in your capability adoption, displaying your current adoption percentage rating for each metric as well as a comparison against industry averages. With deep insight into how you are leveraging prevention capabilities, you can continuously improve your security.

The BPA Executive Summary is designed for management and executives to better understand the current state of security capability adoption at a glance—including information on progress from prior reports, if available—to help your organization confidently progress toward best practice implementation.

Frequently Asked Questions

How does the BPA relate to industry and regulatory standards, such as the NIST framework?

You can view your BPA results mapped to the control categories of industry standards. Gain confidence in your controls by seeing your BPA results in relation to security controls frameworks important to your organization (e.g., ISO, HIPAA, COBIT, NIST, CIS, CISSP).

How do I run a BPA?

Access a self-service BPA from the Customer Support Portal, contact your sales representative, or request a BPA here.

How often should I run a BPA?

You can run a BPA as often as you like. We recommend doing so at least every 90 days or whenever there has been a significant change on your network.

You can learn more about the BPA on our website.

About Palo Alto Networks

Palo Alto Networks, the global cybersecurity leader, is shaping the cloud-centric future with technology that is transforming the way people and organizations operate. Our mission is to be the cybersecurity partner of choice, protecting our digital way of life. We help address the world's greatest security challenges with continuous innovation that seizes the latest breakthroughs in artificial intelligence, analytics, automation, and orchestration. By delivering an integrated platform and empowering a growing ecosystem of partners, we are at the forefront of protecting tens of thousands of organizations across clouds, networks, and mobile devices. Our vision is a world where each day is safer and more secure than the one before. For more information, visit www.paloaltonetworks.com.

BPA Resource Links

- Customer Support Portal: https://support.paloaltonetworks.com/Support/Index
- Request a BPA: https://start.paloaltonetworks.com/best-practice-take-the-next-step-to-better-security
- Learn more about the BPA: https://www.paloaltonetworks.com/services/bpa

paloalto NETWORKS

3000 Tannery Way
Santa Clara, CA 95054

Main: +1.408.753.4000
Sales: +1.866.320.4788
Support: +1.866.898.9087

www.paloaltonetworks.com

© 2020 Palo Alto Networks, Inc. Palo Alto Networks is a registered trademark of Palo Alto Networks. A list of our trademarks can be found at https://www.paloaltonetworks.com/company/trademarks.html. All other marks mentioned herein may be trademarks of their respective companies.
best-practice-assessment-b-041620