BEST PRACTICE ASSESSMENT FOR NGFW AND PANORAMA

Q: What is the Best Practice Assessment for NGFW and Panorama?

A: The Best Practice Assessment (BPA) for NGFW and Panorama consists of two components: the Best Practice Assessment itself and the Security Policy Capability Adoption Heatmap.

The BPA assesses configurations, identifies risks, and provides recommendations on how a customer can remediate issues. It compares a customer's current configurations against best practices and produces a guide to which best practices the customer is and isn't following, including detailed recommendations per feature. The report's summary view covers security controls aligned with various best practice checks, such as the CIS Critical Security Controls and NIST Framework.

Adoption Heatmaps analyze Panorama management and individual NGFW configurations to produce a visualization of how customers are taking advantage of our prevention capabilities. Specifically, the tool analyses a customer's rule base to identify whether the customer is using our capabilities where relevant. Shown in a matrix form along with color coding, this information can be an effective way to start adoption discussions with your customers about their existing deployments. The Trending tab in the heatmap provides a good indication of how a customer's security posture is progressing over time.

Q: How do I generate a BPA?

A: To generate a BPA, follow these steps:

(1) Request the "tech support file" from the Operations/Support tab of the NGFW and/or Panorama.

(2) As a partner, you have two options to generate a BPA:

  a. **Partner Portal:** Select a registered opportunity in the NextWave Portal. Navigate to the Security Lifecycle Review section of the opportunity page, and click the "Create BPA Report" button. You'll be redirected to the Customer Success portal where you can upload the tech support file (the .tgz.gz file only) to the tool.

  b. **Customer Success Site:** Navigate to the Customer Success Site and upload the tech support file to the tool.

(3) Map the zone type and area of architecture to each zone.

(4) Create and confirm a password for the BPA .zip file.

(5) Download the password-protected BPA .zip file.

Q: How long does it take to generate the BPA?

A: The tech support file upload process can take longer on slower connections, but once the file is successfully uploaded, parsing takes fewer than 20 seconds.

Q: Is the tech support file saved on the server after it is uploaded?

A: No, the tech support file is deleted immediately after the BPA is generated.

Q: Is any of the BPA or heatmap data stored in a database?

A: Yes, we store metadata to track adoption trends and industry benchmarks. However, we do not store rule details or any sensitive customer information. Please refer to the BPA Privacy Datasheet to see how we process customer files and maintain them securely.

Q: How can users view a list of all previous BPAs they have generated?

A: Navigate to customersuccess.paloaltonetworks.com/bpa to view a table of all previous reports. You can also archive old reports.

Q: Why is it important to map the area of architecture to each zone?

A: When we map zones to an area of architecture, the customer can better understand the necessity and business purpose of each zone. This also helps ensure profiles are applied consistently across all areas of architecture. Most importantly, it helps in filtering policies between different source and destination areas of architecture. This gives a better view of capability adoption and helps determine if the level of adoption is what was expected or if there are gaps in the customer's security posture.

Q: Why is the adoption zero percent for the heatmaps?

A: Zero percent adoption indicates a security profile or feature is not enabled in the customer's security policies. Customers may keep it that way because they are not using a particular capability. For example, URL Filtering adoption can be zero percent on a data center firewall rule—URL Filtering may not be needed for internal firewalls or those that never process traffic to/from the internet—but it may be 90% on a perimeter firewall rule.

Q: Who came up with the best practice logic?

A: The logic behind the best practice checks in the BPA comes from a group of individuals from various areas of Palo Alto Networks, including ETAC, Professional Services, Global Practice, Support, Customer Experience, Product Management, and Business Development. The scope of the exercise was to go through nearly every feature of PAN-OS to document, from a prevention perspective, how a customer would properly configure each one.

Q: How, and by whom, are the best practices maintained and updated?

A: Our Customer Experience Automation team centrally maintains the best practice logic. Updates to existing best practice checks or requests for new checks come from our users. We encourage all users to provide feedback at: bpa@paloaltonetworks.com.

Q: Are the best practices in AutoAssistant and the BPA the same?

A: Yes, AutoAssistant and the BPA use the same central Python library that parses XML configurations to perform each best practice check. We work with the AutoAssistant development team to ensure they always have the latest version of code to align the logic.

Q: Are the best practices in Expedition migration tool and the BPA the same?

A: Yes, Expedition and the BPA use the same central Python library that parses XML configurations to perform each best practice check. We work with the Expedition development team to ensure they always have the latest version of code to align the logic.

Q: Why can't users dismiss a failed best practice check in the HTML report for the BPA?

A: The BPA HTML report is a static document with no back-end data persistence layer. Although having this functionality in the HTML report is technically possible, any dismissed failed checks cannot be saved and subsequently shared. To get around this limitation, we have a secondary Excel file that provides the list of all failed best practice checks. An internal employee, customer, or partner can use this file to track progress on the remediation of failed best practice checks.

Q: Where can I access the documentation of the best practices themselves?

A: You have three options for viewing documentation of best practices:

(1) Within the BPA HTML report by clicking the "?" icon in each section of the report.

(2) In the secondary Excel file of failed best practice checks.

(3) On the Customer Success Portal at customersuccess.paloaltonetworks.com/bpa/documentation.