

Palo Alto Networks' (PAN) Best Practice Assessment (BPA) is a meticulous, accessible, and cost-effective assessment that provides visibility into your PAN implementation while identifying areas of opportunity to improve your secure posture within the platform. Combining the PAN BPA with Trace3's Security services supports reducing risk and updating key configurations based on prioritized discovery findings.



WHY BPA IS CRITICAL FOR PAN SUCCESS?

INCREASE VISIBILITY WITH ADVANCED SECURITY CONTROLS

Measure your security capabilities with customizable heatmap reports and industry benchmarks.

REDUCE THREAT VECTORS

Reduce opportunities for attack by creating usage baselines and systematically decreasing unnecessary applications and user traffic.

IMPROVE SECURITY OPERATIONS IN REAL-TIME VIA COMMAND LINE INTERFACE (CLI)

Stay up to date on the effectiveness of controls by repeating the assessment regularly and demonstrating increased prevention capabilities by using the BPA+ CLI wizard.

PAN BPA BENEFITS



Document your existing Palo Alto Firewall Security settings.



Measure your firewall's position against Palo Alto's high standards.



Identify areas for improvement, and their criticality to current industry standards.



Develop a plan to remediate and harden your current PAN security posture.

TRACE3 PAN EXPERTISE

- Trace3's PAN engineers help clients build and mature cybersecurity policies that protect organizational networks.
- Trace3 reviews your current PAN configuration, gains an understanding of what is being used today, determines items relevant to your environment and policies, and develops an observation log based on BPA findings and your related concerns.
- Trace3 prioritizes identified gaps and opportunities in terms of severity for remediation and then leads your team through a comprehensive PAN BPA briefing .
- Trace3 tailors services to remediate the BPA findings.

TRACE3 BPA BUNDLED REMEDIATION SERVICES

As part of the PAN BPA engagement, Trace3 engineers will provide remediation services from the following options: Levels of Security:

Transformation Level 1 – General Visibility – Non-Encrypted Traffic

- Layer 3/4 policy migration
- Threat prevention, URL filtering, and WildFire enabled in alert mode
- Decryption strategy created

Transformation Level 2 – Medium Level Control – Reduce Attack Surface On All Traffic

- Layer 7 policy creation
- Block unsanctioned applications
- Threat prevention, URL filtering, and WildFire enabled in block mode

Transformation Level 3 – Advanced Security Policy Enforcement

- Policy evolution and enhancement
- Application and user segmentation
- Last-mile threat analysis, tuning, recategorization, and blocking
- Decryption strategy optimized
- AutoFocus, MineMeld, Magnifier deployed

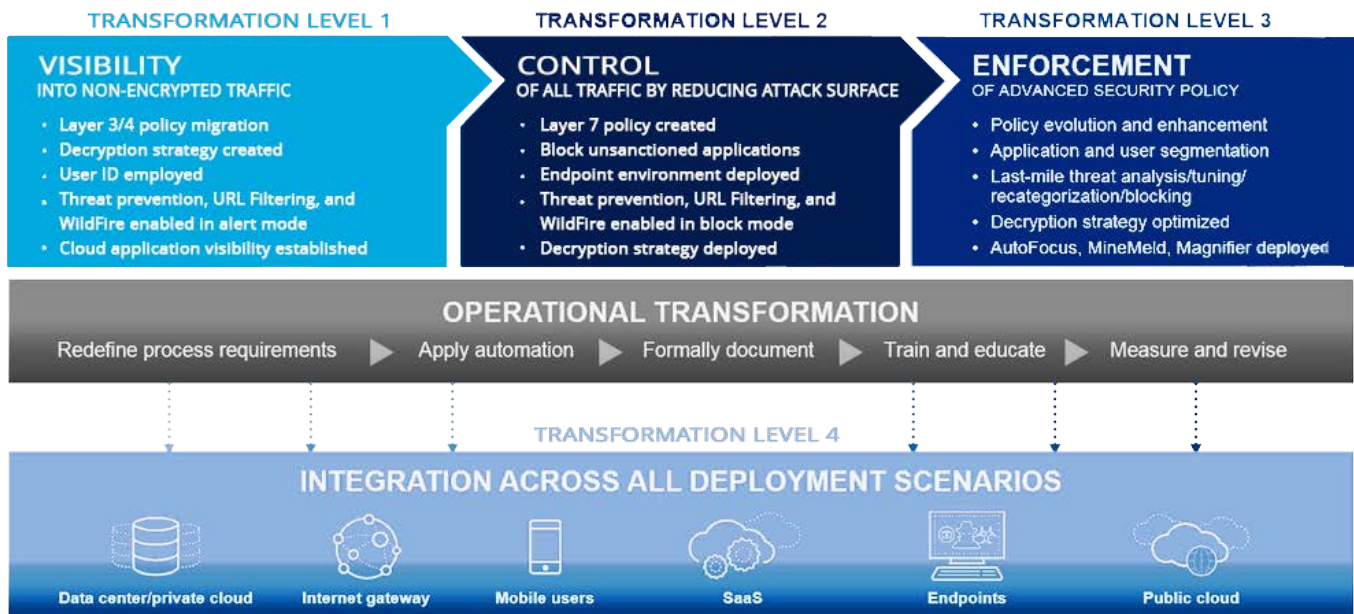
Transformation Level 4 - Integration Across All Deployment Scenarios

- Data center/private cloud
- Internet gateway
- Mobile users
- SaaS
- Endpoints
- Public cloud

Load Balancing Options

Verify, validate, and configure load balancing methods:

- IP Module
- IP Hash
- Round Robin
- Weighted Round Robin



To schedule a Best Practice Assessment or learn more about our security initiatives, contact your Trace3 Sales Representative or find us at [Trace3.com](https://www.Trace3.com).