Getting Started with the BPA
9.0
Table of Contents

Evaluate Security Policy Capability Adoption.............................................. 5
  Review the Adoption Summary...............................................................................................................7
  Identify Gaps in Adoption.........................................................................................................................9
  Identify Rules to Improve....................................................................................................................... 13

Evaluate Best Practice Configuration.......................................................... 15
  Review the Best Practice Summary..................................................................................................... 17
  Review Best Practice Policy Configuration........................................................................................ 19
  Review Best Practice Objects Configuration......................................................................................... 20
  Review Best Practice Network Configuration....................................................................................... 21
  Review Best Practice Device and Panorama Management Configuration........................................... 22

Prioritize Best Practice Changes...................................................................23
  Strengthen Device Management Posture............................................................................................... 25
  Improve Visibility into Traffic................................................................................................................ 26
  Implement Initial Best Practice Controls............................................................................................... 28
  Fine-Tune and Enhance Best Practice Controls..................................................................................... 29
Evaluate Security Policy Capability Adoption

The Best Practice Assessment (BPA) tool helps you understand your current level of Security policy capability adoption and helps you assess the maturity and effectiveness of your security posture. Adopting capabilities such as WildFire, Vulnerability Protection, SSL Decryption, etc., contributes to detecting and preventing attacks. Developing a solid understanding of how and where to use each capability in different environments is critical to understanding how to best protect your network and its valuable assets.

Getting Started with Best Practices shows how to access and run the BPA. The Capability Adoption Heatmaps section of the BPA report enables you to review the adoption of these capabilities across the Security policy rulebase. Watch the Introduction to Heatmaps video to learn about Heatmaps, and take advantage of the BPA video library to learn more about the tool.

Review and analyze the information on the Heatmap tabs to identify gaps in security capability adoption and determine what you want to improve:

- Review the Adoption Summary
- Identify Gaps in Adoption
- Identify Rules to Improve
Review the Adoption Summary

After you or your Palo Alto Networks representative runs the BPA, the resulting HTML report opens on the Heatmap page, in the Adoption Summary. The Adoption Summary view provides an overview of your device’s overall adoption of security capabilities. The report shows the current adoption percentage for each metric (except Industry Average, which provides the adoption averages in your industry to compare against your adoption), and in parentheses, the percentage change in adoption since the last time you ran the BPA on the device’s configuration file (or No change if the value is the same as the last time you ran the BPA).

**Overall Adoption**—Adoption of Security profiles in Security policy allow rules. Percentages are based on the number of allow rules that have one or more profiles enabled as part of the rule. The BPA doesn’t count disabled rules or block rules.

**Industry Average**—Average adoption of Security profiles in allow rules for your company’s industry.

**Best Practice Mode**—Adoption of Security profiles configured in the recommended best practice manner in allow rules. The BPA only counts rules with profiles that pass all best practice checks.

**App-ID Adoption**—Adoption of App-ID across Security policy rules. The percentage value is based on the total number of allow rules with one or more defined application (the Application is not any). The BPA doesn’t count disabled rules.

**User-ID Adoption**—Adoption of User-ID across Security policy rules. The percentage value is based on the total number of allow rules with users (including the values known-user and unknown) or user groups. The BPA doesn’t count disabled rules.
**Service/Port Adoption**—Adoption of service/port across Security policy rules. The percentage value is based on the total number of allow rules with a defined service or port (the Service is not any). The BPA doesn’t count disabled rules.

The BPA doesn’t count App-ID, User-ID, or Service/Port adoption for block rules because the rationale for blocking differs from business to business, so the BPA can’t make recommendations based on block rules.

**Logging Adoption**—Adoption of Log at Session End across Security policy rules. The percentage value is based on the total number of rules with Log at Session End enabled. The BPA doesn’t count disabled rules.

**Log Forwarding Adoption**—Adoption of Log Forwarding profiles across Security policy rules. The percentage value is based on the total number of rules with a Log Forwarding profile configured. The BPA doesn’t count disabled rules.

**Zone Protection Adoption**—Adoption of Zone protection across Security policy allow rules. The percentage value is based on the total number of allow rules in which the source zone has a Zone Protection profile configured. The BPA doesn’t count disabled rules.

For each of these metrics, the value in parentheses next to each percentage is the percentage change in adoption since the last time you ran the BPA on the device’s configuration file (or No change if the value is the same as the last time you ran the BPA).

**Decryption Summary**—Shows if the configuration includes Decryption policy rules for SSL Forward Proxy, SSL Inbound Inspection, and SSH Proxy. The summary also shows if the configuration includes Decryption profiles and identifies URL categories that the device exempts from decryption.

If you don’t decrypt a URL category, you can’t inspect its traffic because the firewall can’t see what’s inside the encrypted traffic. The firewall can only inspect traffic you decrypt.

Next: Identify Gaps in Adoption to understand where you can improve security.
Identify Gaps in Adoption

The Heatmap shows where your security policy is strong and where there are gaps in security policy capability adoption that you can focus on improving. To gain maximum visibility into traffic and maximum protection against attacks, set goals for security capability adoption and use the following recommendations as a best practice baseline. Assess your current posture against the baseline to identify gaps in security policy capability adoption.

Heatmaps help identify devices, zones, and areas where you can improve security policy capability adoption. You can review adoption information by Device Group, Serial Number & Vsys, Zones, Areas of Architecture, and Tags. Column Filters filter on device groups, devices, zones, areas of architecture, and tags to narrow the scope and identify gaps.

In the Heatmap’s Security Profile Adoption Summary, check the adoption rates of the following capabilities and use the recommendations as gap identification criteria—if the actual adoption rate doesn’t match the recommendations, plan to close the gap.:
Apply WildFire, Antivirus, Anti-Spyware, Vulnerability Protection, and File Blocking security profiles to all allow rules, with a target of 100% or almost 100% adoption. If you don’t apply a profile to an allow rule, ensure there is a good business reason not to apply the profile.

Configuring security profiles on all allow rules enables the firewall to inspect all decrypted traffic for threats, regardless of application or service/port. After updating the configuration, run the BPA to measure progress and to catch new rules that don’t have security profiles attached.

You can apply WildFire profiles to rules without a WildFire license. Coverage is limited to PE files, but this still provides useful visibility into unknown malicious files.

In the Anti-Spyware profile, apply DNS Sinkhole to all rules to prevent compromised internal hosts from sending DNS queries for malicious and custom domains, to identify and track the potentially compromised hosts, and to avoid gaps in DNS inspection. Enabling DNS Sinkhole protects your network without affecting availability, so you can and should enable it right away.

Apply URL Filtering and Credential Theft (phishing) Protection to all outbound internet traffic.

In the Heatmap’s Application & User Control Adoption Summary, check the adoption rates of the following capabilities. Use the recommendations as gap identification criteria—if the actual adoption rate doesn’t match the recommendations, plan to close the gap:

- Apply App-ID to as close to 100% of the rules as possible. Apply User-ID to all rules with source zones or address ranges that have a user presence (some zones may not have user sources; for example, sources in data center zones should be servers and not users). Leverage App-ID and User-ID to create whitelist (allow rule) policies that allow appropriate users to sanctioned (and tolerated) applications. Explicitly block malicious and unwanted applications.
Target 100% or close to 100% service/port adoption—don’t allow applications on non-standard ports unless there’s a good business reason for it.

In the Heatmap’s Logging & Zone Protection Adoption Summary, check the adoption rates of the following capabilities. Use the recommendations as gap identification criteria—if the actual adoption rate doesn’t match the recommendations, plan to close the gap:

- Target at or close to 100% adoption for Logging and Log Forwarding.
- Configure Zone protection profiles on all zones.

In summary:

<table>
<thead>
<tr>
<th>Feature</th>
<th>Adoption Goal</th>
</tr>
</thead>
<tbody>
<tr>
<td>WildFire</td>
<td>As close to 100% of Security policy rules as possible</td>
</tr>
<tr>
<td>Antivirus</td>
<td>As close to 100% of Security policy rules as possible</td>
</tr>
<tr>
<td>Anti-Spyware</td>
<td>As close to 100% of Security policy rules as possible</td>
</tr>
<tr>
<td>Vulnerability</td>
<td>As close to 100% of Security policy rules as possible</td>
</tr>
<tr>
<td>File Blocking</td>
<td>As close to 100% of Security policy rules as possible</td>
</tr>
<tr>
<td>URL Filtering and Credential Theft</td>
<td>All outbound internet traffic</td>
</tr>
<tr>
<td>App-ID</td>
<td>As close to 100% of Security policy rules as possible</td>
</tr>
<tr>
<td>User-ID</td>
<td>All rules with source zones or address ranges that have a user presence</td>
</tr>
<tr>
<td>Service/port</td>
<td>As close to 100% of Security policy rules as possible</td>
</tr>
<tr>
<td>Logging</td>
<td>As close to 100% of Security policy rules as possible</td>
</tr>
<tr>
<td>Log Forwarding</td>
<td>As close to 100% of Security policy rules as possible</td>
</tr>
<tr>
<td>Zone protection</td>
<td>All zones</td>
</tr>
</tbody>
</table>

Use Column Filters to narrow the scope. Use the resulting information to identify gaps in security policy capability, measure against gap identification criteria, and refine or establish new gap identification criteria.
for further investigation. For example, to create a filter that displays adoption of rules that control traffic to the internet Area of Architecture:

**STEP 1** | In the Heatmaps section of the BPA, click Areas of Architecture.

**STEP 2** | Click Column Filters to expand the filter options.

**STEP 3** | Set the Destination Area of Architecture to Internet.

**STEP 4** | Click Apply Filters.

The BPA filters the results:

Interpret the results based on your security goals and criteria. For example, if your goal is to apply WildFire to 100% of your allow rules, the filtered Heatmap reveals that only 50% of your DMZ allow rules have WildFire profiles, so you have identified a gap to target for improvement.

**STEP 5** | Next: Identify Rules to Improve.
Identify Rules to Improve

After you identify a gap in security policy capability adoption, use the Rule Detail view to list rules that require further investigation or remediation. Configure Column Filters to match the gap identification criteria you developed when you identified gaps in adoption. This results in rule lists you can export and hand off to the operational team in charge of firewall Security policy.

For example, to create a Rule Detail filter to identify rules that allow all traffic and don’t have a Vulnerability Protection profile configured:

**STEP 1** | In the Heatmaps section of the BPA, click Rule Detail.

**STEP 2** | Click Column Filters to expand the filter options and then select the following filters:

- Source Zone = any
- Destination Zone = any
- Source Address Configured = No
- Destination Address Configured = No
- Action = allow
- Rule Enabled = Yes
- Vulnerability On = No

**STEP 3** | Click Apply Filters.

The BPA lists the rules that match the filters:
STEP 4 | To export the filtered rule list to a .csv file, click **Export Data**.

STEP 5 | **Next:** Evaluate Best Practice Configuration.
Evaluate Best Practice Configuration

The Best Practice Assessment (BPA) tool helps you understand the current level of best practice configuration in your Security policy so you can assess the maturity of your security posture. Watch the Introduction to the BPA video to learn about the BPA, and take advantage of the BPA video library to learn even more about the tool.

When you first open the BPA report, it opens in the Heatmap section. Click Go to Best Practice Assessment to go to the BPA section of the report, which focuses on the adoption of configuration best practices for next-generation firewalls and Panorama.

In addition to this documentation, you can view the BPA demo and a short video about how to run a BPA to learn more about using the BPA.

A BPA report evaluates a next-generation firewall or Panorama configuration file against more than 200 best practice checks. The BPA groups the results of the evaluation by policies, objects, network, and device/Panorama information, similar to the PAN-OS user interface. Review and analyze the information to find areas to focus on and improve:

> Review the Best Practice Summary
> Review Best Practice Policy Configuration
> Review Best Practice Objects Configuration
> Review Best Practice Network Configuration
> Review Best Practice Device and Panorama Management Configuration
Review the Best Practice Summary

When you change the view from Heatmaps to the BPA report, the report shows you the Best Practice Summary.

The summary presents best practice configuration check results mapped to the control categories of industry standards, such as the Center for Internet Security’s (CIS) Critical Security Controls and the National Institute of Standards and Technology (NIST) publication on Security Controls and Assessment Procedures. The purpose of this information is to provide a good way to learn how BPA checks tie to industry standards, not to act as an audit.

Like the Adoption Summary, the Best Practice Summary includes metrics that show your current adoption rate and adoption progress (in parentheses) since the last time you generated the BPA on the device’s configuration.

Click Mapping Definitions (left sidebar) to see a complete list of all of the mapped checks and their individual scores. Show Filters to set filters, Apply Filters to the output, and Export Mappings to export the mappings to a .csv file.
Next: Review Best Practice Policy Configuration.
Review Best Practice Policy Configuration

The **Policies** tab shows all checks related to different types of firewall policies. Select the type of policy you want to review to identify potential rule improvements. The **Security** policy view displays rule-based check results (**Security Rule Checks**). **Show Filters** to configure filters that narrow the results to rules that failed one or more particular checks. You can **Export Data** to export the list to a .csv file for remediation analysis.

Click help (?) to view the description of and rationale for each check, along with a link to technical documentation about the capability each check examines.

Below the **Security Rule Checks**, the **Security Rulebase Checks** summarize the best practice check results by device group, with a pass/fail status and recommendations for what to do about failed checks. Click help to view the description of and rationale for each result, along with a link to technical documentation.

When you review **Policy** information, at a minimum, review the following items to help understand the scope of policy remediation (switch between views):

- **Security**—Identify rules that fail the **Source/Destination != any/any** check.
- **Security**—Identify rules that fail the **App-ID with Service** check.
- **Security**—Identify User-ID rules that fail the **User-ID Rules without User ID enabled on Zone** check.
- **Decryption Rulebase**—SSH Proxy decryption checks.
- **Decryption**—Each Decryption policy rule should have an associated Decryption profile.
- **Application Override**—Application Override rules that use a simple custom application bypass Layer 7 inspection for matching traffic. Reduce or eliminate Application Override rules that use a simple custom application so you can **Improve Visibility into Traffic** and inspect the applications and content these rules control.

Next: **Review Best Practice Objects Configuration**.
Review Best Practice Objects Configuration

The **Objects** tab shows all checks related to different types of firewall objects. Select the type of object you want to review to understand the existing configuration and to identify potential gaps in best practice configuration related to Tags, GlobalProtect, Security profiles, Log Forwarding, and Decryption profiles. The following example shows the result for an Antivirus Security profile.

For each profile, the report shows the current configuration and how many rules use the profile. The report shows the best practice check results below the current configuration with pass/fail status and recommendations for failed best practice checks. Click help for the rationale for each check and links to best practice documentation.

When one or more checks fail, the profile title turns red. The report lists profiles that aren't in use at the bottom with a yellow title.

When you review the **Objects** tab, at a minimum, review the following items to help understand the potential scope of remediation:

- **Antivirus**—Decoder actions for both Antivirus and WildFire.
- **Anti-Spyware**—Strict Profile, DNS Sinkhole.
- **Vulnerability Protection**—Strict Profile.
- **URL Filtering**—Whether known bad categories are blocked.
- **WildFire Analysis**—Profile File Types (all types should be sent to WildFire for analysis).
- **Log Forwarding**—Whether all log types are forwarded (forward all log types).

Next: Review Best Practice Network Configuration.
Review Best Practice Network Configuration

The **Network** tab shows all checks for network-related configuration. On the left nav, select the network check you want to review to understand the existing configuration and to identify potential gaps in best practice configuration related to Zones, GlobalProtect, IPsec Crypto, and Zone Protection profiles. The following example shows the result for Zones.

The report shows the current configuration for each item. The best practice check results for each item appears below its current configuration. You can specify a **Device Group** and/or **Template** to limit the scope of the information displayed.

Each check has pass/fail status and recommendations for failed best practice checks. Click help for the rationale for each check and links to best practice documentation. When one or more checks fail, the item’s title turns red.

When you review the **Network** tab, at a minimum, review the following items to help understand the potential scope of remediation:

- **Zones**—Whether each zone has Packet Buffer Protection enabled and has a Zone Protection profile.
- **Zone Protection**—Whether Flood Protection and Packet-Based Attack Protection are enabled.

Next: Review Best Practice Device and Panorama Management Configuration.
Review Best Practice Device and Panorama Management Configuration

The **Device** and **Panorama** tabs show all checks related to device management configuration. Select the device management check you want to review to understand the existing configuration and to identify potential gaps in best practice configuration related to firewall and Panorama device management. The following example shows the result for General Settings for the firewall (click **Panorama** to see the Panorama check results).

The report shows the current configuration for each item. The best practice check results for each item appears below its current configuration. When viewing information for a **Device**, you can specify a **Template** to limit the scope of the information displayed.

Each check has pass/fail status and recommendations for failed best practice checks. Click the question mark for the rationale for each check and links to best practice documentation. When one or more checks fail, the item’s title turns red.

When you review the **Device** or **Panorama** tab, at a minimum, review the following items to help understand the potential scope of remediation:

- **Dynamic Updates**—Antivirus, Apps, Threats, and WildFire updates.
- **Management Interface Settings**—Network Connectivity Services, Permitted IP Addresses.
- **Administrators**—Local Admins, Administrator Password profile. Check **Device > Administrators** or **Panorama > Administrators** to ensure Administrators’ passwords are configured with the minimum required complexity.
- **Minimum Password Complexity**—Password minimum complexity requirements check.

Next: Prioritize Best Practice Changes.
Prioritize Best Practice Changes

The amount of information in a BPA report can be overwhelming. This chapter provides recommendations to help you prioritize improvement to your configuration so you can close security gaps, implement the highest-value enhancements first, and make progress toward achieving a best practice security posture.

The following topics focus on how to improve your security posture in the order in which new deployments are usually implemented, focusing on management first, then visibility, control, and enforcement. Existing deployments already may have achieved some maturity in each area.

> Strengthen Device Management Posture
> Improve Visibility into Traffic
> Implement Initial Best Practice Controls
> Fine-Tune and Enhance Best Practice Controls
Strengthen Device Management Posture

Strengthening your device management posture secures the firewall by preventing unauthorized access that could compromise it, reduces the operational impact of unexpected events, and provides greater visibility into firewall operation.

- Follow the best practices for securing administrative access to prevent unauthorized and unsecured access to the device’s management interface.
- Forward all system and configuration logs to Panorama and to third-party monitoring solutions to keep track of system-related events and configuration changes.
- Create a configuration backup schedule so you can remediate configuration-related issues and system outages faster.

After you configure changes, Run the BPA to validate the changes, measure progress, and prioritize the next changes.

Next: Improve Visibility into Traffic.
Improve Visibility into Traffic

You can’t protect yourself against threats you can’t see, so you must ensure you have full visibility into traffic, across all users and applications, at all times. Complete visibility into the applications, content, and users on your network is the first step toward informed policy control:

- Maximize Security profile adoption. After you Review the Adoption Summary and identify gaps in adoption, remediate the gaps using the safe transition steps to move toward a full best practice Security profile implementation.

- Maximize Logging adoption (including Log Forwarding) across the Security policy rulebase to inspect all traffic.

- Configure best practices for dynamic content updates to ensure the firewall has the latest application and threat signatures to protect your network and that you deploy updates based on your network security and availability requirements.

- Plan your SSL Decryption deployment based on best practices.

- Enable User-ID in user zones (internal, trusted zones from which users initiate traffic) to map application traffic and associated threats to users and devices.

  Don’t enable User-ID in external untrusted zones. If you enable User-ID (or client probing such as WMI) on an external untrusted zone, probes could be sent outside your protected network and expose User-ID information such as the User-ID Agent service account name, domain name, and encrypted password hash, which could enable an attacker to compromise your network.

- Reduce or eliminate Application Override rules so you can inspect the applications and content these rules control (an Application Override rule is a layer 4 rule that doesn't allow the firewall to inspect the traffic). Eliminate the need for or reduce the scope of basic Application Override rules:

  - Validate whether the use case for the rule still exists. Often, an Application Override rule was created to overcome a specific issue related to performance, protocol decoders, or unknown applications. Over time, PAN-OS updates, content updates, or hardware upgrades may remove the need for some Application Override rules. If you run PAN-OS 9.0 or later on firewalls or PAN-OS 9.0 or later on a Panorama managing firewalls running PAN-OS 8.1 (or later), you can use Policy Optimizer to transform the rule to a layer 7 rule.

  - Reduce the scope of the Application Override rule so it only affects the minimum possible amount of traffic. Rules that are defined too broadly may override more traffic than necessary or intended. Define source and destination zones, address, and/or ports in each Application Override rule to limit the rule's scope as much as possible.

  - Create layer 7 custom applications for internal applications.

  - Create Service objects with custom timeout values.

- Plan to deploy DoS and Zone Protection and take baseline CPS measurements so you can set reasonable flood protection thresholds.

When you implement these native App-ID, Content-ID, User-ID, and SSL Decryption capabilities, the firewall gains visibility into and can inspect all of your traffic—applications, threats, and content—and tie events to the user, regardless of location, device type, port, encryption, or an attacker’s evasive techniques.

Improving the adoption of capabilities such as SSL Decryption, logging, flood protection, Security profiles, etc., may result in additional firewall resource consumption. Understand the capacity of your firewalls and ensure they’re properly sized to handle any additional load. Your Palo Alto Networks SE or CE can help you size the deployment. You also may need additional log storage space.
After you configure changes, Run the BPA to validate the changes, measure progress, and prioritize the next changes.

Next: Implement Initial Best Practice Controls.
Implement Initial Best Practice Controls

After you gain visibility and context into the traffic on your network—applications, content, threats, and users—implement strict controls to reduce the attack surface and prevent known and unknown threats to complete the transition to a best practice configuration.

- After you Review the Adoption Summary and identify gaps in adoption, follow the safe transition steps to move toward best practice Security profiles to block threats and reduce the attack surface, including implementing strict controls in the data center to protect the most valuable assets of your business.
- Create application-based Security policy rules for data center and perimeter firewalls; use the perimeter firewall best practice recommendations for other firewalls that aren’t in the data center. If you run PAN-OS 9.0 or later on firewalls or PAN-OS 9.0 or later on a Panorama managing firewalls running PAN-OS 8.1 (or later), you can use Policy Optimizer to convert port-based rules to application-based rules.
- Create user-based access policies.
- Deploy best practice Zone Protection profiles to all zones.
- Deploy SSL Decryption so the firewall can gain visibility into (decrypt) and inspect encrypted traffic.

After you implement control capabilities, the firewall can scan all allowed traffic and detect and block network and application-layer vulnerability exploits, buffer overflows, DoS attacks, port scans, and known and unknown malware variants. The firewall controls application and user access as well as blocking malicious and unwanted applications.

After you configure changes, Run the BPA to validate the changes, measure progress, and prioritize the next changes.

Next: Fine-Tune and Enhance Best Practice Controls.
Fine-Tune and Enhance Best Practice Controls

After you implement control over your network traffic—applications, content, threats, and users—start fine-tuning the controls and implement additional functionality to improve your security posture.

- If you haven’t converted internal applications to custom applications to gain visibility into and control of the traffic, convert internal applications to custom applications.
- Tune Security profiles to best practices after you use the safe transition steps to begin the move to best practice profiles.
- Block known malicious IP addresses based on threat intelligence from Palo Alto Networks and reputable third-party feeds.
- Deploy GlobalProtect or GlobalProtect Cloud Service to extend the next-generation security platform to users and devices regardless of where they are located.
- Enable credential theft prevention.
- Configure network-based Multi-Factor Authentication.

Next: Run the BPA to validate changes, measure progress, and prioritize the next changes, learn more about best practices, and learn more about the many security capabilities of Panorama and PAN-OS next-generation firewalls.