

Palo Alto Networks and BackBox Integrated Network Security Solution

Continuously Maintain and Improve
Network Security Posture

Integration Highlights

- Automated OS upgrades and patches for all network devices from Palo Alto Networks and other vendors across your network infrastructure in a timely manner to maintain security posture.
- Automated backup of the latest configuration of Palo Alto Networks NGFW and Panorama devices. Self-verification mechanism of BackBox ensures configuration backup files validity.
- Easily restore device configuration with 'single-click' disaster recovery to minimize downtime of your Palo Alto Networks NGFW.
- Automated remediation of discovered compliance conflicts or security vulnerabilities of Palo Alto Networks NGFW configuration to comply with organization or industry/government policies or standards.
- Monitor device performance and status of Palo Alto Networks NGFW and other network devices to predict possible outages so that proactive actions can be taken as preventive measures.
- Automated discovery of all Palo Alto Networks NGFW and other devices connected to the network for tight management of device inventory to comply with cybersecurity standards, such as CIS.

The Challenge

The ongoing risk of network security breaches, and the increase in network complexity with the deployment of hybrid and multi-cloud environments, pose significant challenges to network and security teams.

Vulnerabilities, exploits, and malicious actors continue to add up over time, and outpace the network's ability to keep up in monitoring and mitigating these threats. This results in a constantly weakened security posture which exposes the organization to significant security risk.

Security devices in today's networks are increasingly complex and require constant changes to maximize uptime and maintain the security posture. Administrators are understaffed and under time constraints to manage all tasks under their domain. This leads to potential delays or a neglect of maintenance tasks as workloads become overwhelming. Due to these limitations, even critical tasks are often neglected or overlooked that may cause a higher rate of downtime and slower recovery of these devices.

The Solution

To tackle these challenges, we need a solution that is easy to deploy and maintain with centralized management capabilities; a solution that offers complete visibility and security across different network infrastructure, both on-premises and in the cloud environment; and a solution that automates the process of continuously validating and improving network security posture.

BackBox and Palo Alto Networks NGFW & Panorama Devices Integrated Solution

BackBox offers automated backup and recovery of Palo Alto Networks NGFW and Panorama network security management devices, minimizing downtime when recovery is needed.



BackBox can help ensure Palo Alto Networks NGFWs are up and running at optimal performance efficiency.

BackBox also collects asset information from Palo Alto Networks NGFWs and Panorama across the network and then reports on inventory information, including license information, device model, serial number, and more.

With its unique device health check, BackBox can help ensure Palo Alto Networks NGFWs are up and running at optimal performance efficiency.

BackBox provides a foundation to harmonize the configuration between multiple devices, enabling seamless integration to meet specific organization or industry standards and requirements. For example, users can track Palo Alto Networks NGFWs and ensure they align with industry compliance standards or organizational guidelines. Users can also employ BackBox to track configuration changes and differences from the baseline.

BENEFITS OF THE INTEGRATION:

- Automated, verified PAN-OS upgrades to maintain network security posture.
- Automated configuration backup for Palo Alto Networks NGFW and Panorama devices.
- Single-click disaster recovery and step-by-step disaster recovery procedures.
- Validation and automatic remediation of configurations against policies and regulations.
- Monitor device performance and status of Palo Alto Networks NGFW.
- Automated discovery of newly connected Palo Alto Networks NGFW for easy asset management.

BackBox Intelligent Network Security Automation

BackBox is designed for complex, hybrid, multi-cloud, and multi-vendor networks. With BackBox, network and security teams can save time and deliver better and more secured IT services.

BackBox offers a simple way to intelligently automate the backup, restoration, and management of all devices on a network by providing centralized management of devices such as firewalls, routers, switches, and load balancers. Each of these devices plays a critical role in the availability and security of an organization's network, and BackBox ensures they all continue to function effectively and effortlessly, streamlining operations for optimal performance.

Employing centralized management for all device backups also allows BackBox to relay other vital information, such as the status of devices and the network to end users. This lets BackBox assist with predicting when and where outages are more likely to occur, in turn helping organizations prevent such events.

Palo Alto Networks Panorama™ Network Security Management

Panorama™ network security management empowers you with easy-to-implement, consolidated policy creation and centralized management features. Manage your network security with a single security rule base for firewalls, threat prevention, URL filtering, application awareness, user identification, sandboxing, file blocking, access control, and data filtering. This crucial simplification, along with App-ID™ technology-based rules, dynamic security updates, and rule usage analysis, reduces administrative workload and improves your overall security posture.

Use Case 1

CENTRALIZE AND AUTOMATE PAN-OS UPGRADES AND PATCHES

The Challenge:

OS upgrades and patch management is a critical aspect of maintaining network security posture. The versions of OS that runs on the network infrastructure must be closely managed to ensure continuity of service and remediation of known security vulnerabilities. But manually keeping track of the frequent OS upgrades and patches of firewalls and other network and security devices is getting more challenging, especially with limited resources.

The Solution:

BackBox offers automated OS upgrades and patches for Palo Alto Networks NGFW and other security devices across the entire network, eliminating the need for manual tracking, saving time, and helping ensure a hardened network infrastructure. Users can use BackBox to upgrade Palo Alto Networks NGFW's version of PAN-OS security operating system and upgrade hundreds of devices seamlessly with a single click.

Use Case 3

CENTRALIZE AND AUTOMATE PALO ALTO NETWORKS NGFW CONFIGURATION BACKUP

The Challenge:

Manual configuration backup for network security devices like firewalls is time consuming and prone to human errors. In addition to security infrastructure, network engineers must perform regular backups on routers, switches, and other network devices from multiple vendors, via multiple different user interfaces, further increasing risk.

The Solution:

Seamless integration between BackBox and Palo Alto Networks NGFW and/or Panorama enables automated, centralized, and secure backups for all configuration information from Palo Alto Networks devices. This ensures rapid recovery and minimal downtime.

Use Case 2

ENFORCE COMPLIANCE WITH CORPORATE STANDARDS FOR ALL PALO ALTO NETWORKS NGFW AND OTHER SECURITY DEVICES

The Challenge:

With configuration updates getting more frequent due to the acceleration of new threats and malicious actors, it is a challenge to ensure all security devices, such as firewalls, are up-to-date and compliant with internal organization policies and government or industry regulations.

The Solution:

By eliminating the need to manually check device configuration for compliant to organization policies or industry standards, BackBox allows users to easily check for the validity of platform parameters as well as automatically correct them to align with corporate guidelines. Administrators can check Palo Alto NGFW and other network security devices for configuration changes and see the deviation with the baseline.

Use Case 4

MONITOR PERFORMANCE AND STATUS OF PALO ALTO NETWORKS NGFW AND OTHER NETWORK SECURITY DEVICES

The Challenge:

To verify proper network operations and prevent issues from affecting the network, performance information and status of network devices should be checked on a regular basis. But writing automation scripts to perform these tasks could be very time consuming while manually performing these tasks is prone to human errors.

The Solution:

Through centralized management for all network device backups, BackBox collects and relays vital information, such as status of Palo Alto Networks NGFW and other network security devices, to end users. This lets BackBox assist with predicting when and where outages are more likely to occur, in turn helping organizations prevent such events with proactive actions.



About BackBox

BackBox is dedicated to helping our customers continuously improve the health and security of their network infrastructure through intelligent, security-minded automation. We help companies worldwide ensure business continuity, automate complex tasks, achieve and validate compliance, and do more with fewer resources. We believe that network automation should be easy, attainable, and provide our customers with unprecedented time savings and reduced risk.

Find out more at www.backbox.com

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.

For more information, visit www.paloaltonetworks.com

