BACKBOX
SOLUTION BRIEF

paloalto NETWORKS

BackBox Complements Palo Alto Panorama

OS Updates & Vulnerability Patching

Overview

It's common for BackBox to be compared to individual vendor products. As a network automation platform, BackBox can deliver many of the same outcomes as vendor tools like Palo Alto Panorama, Backups and OS Updates for example, but more efficiently and with less risk.

With BackBox two key benefits are achieved with better outcomes than with vendor products, even in single-vendor environments:

- **Teams have increased bandwidth** due to reduced manual work and process benefits that reduce errors.
- **Teams lower the risk of their operating environment** due to updates being done sooner after their release, and reduced manual errors that often cause expensive outages.

Even for single-vendor environments (or the more likely scenario of a single-vendor team inside a multi-vendor environment) BackBox offers feature advantages:

- BackBox automates the end-to-end process and not just the desired outcome (the upgrade or the backup).
- BackBox often supports devices older than the vendor itself supports.
- BackBox automations can be customized in a way that more deeply integrates with the customer environment and delivers a richer outcome.

As an example for point #3, we can chain automations to do pre-and post-checks on a software update to make it more efficient. We'll see this below, when we chain three separate automations together to automate checking for updated signatures, a pre-requisite for completing a device upgrade.

We can also add automated and verified backups before and after an update. Vendor tools cannot do this, even though performing a backup before doing something potentially destructive, like a device update, is an acknowledged best practice.

Let's compare the process of doing a device update using Panorama to what it's like using BackBox.

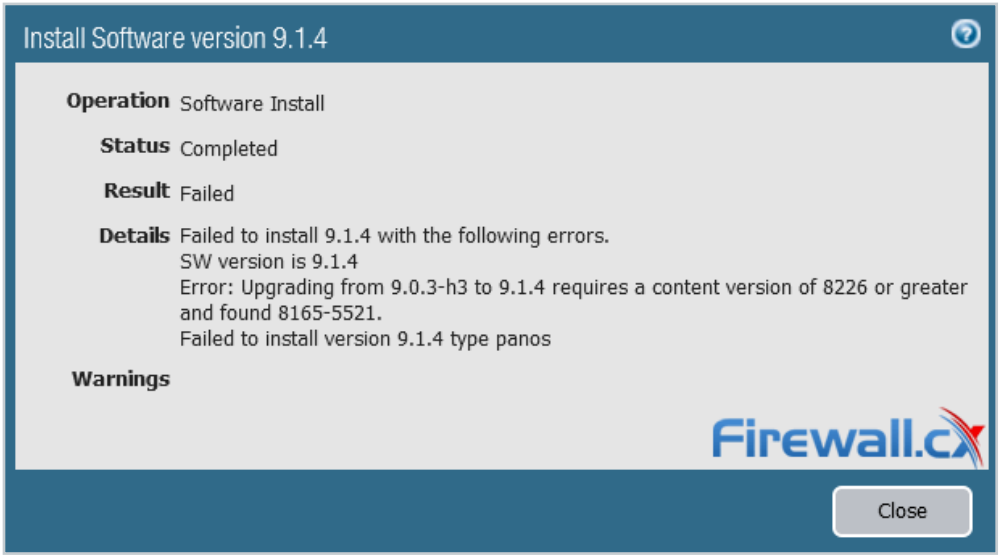
On Panorama

Updating Palo Alto devices is with the Palo Alto GUI.

There are three steps to the upgrade:

1. Update antivirus signatures on the device.
2. Update application and threat signatures on the device.
3. Update the device.

This approach frequently results in the administrator getting an error - either antivirus, or application and threat signatures need updating. If the firewall is connected to the internet it will do these steps automatically, but that only makes things marginally better because of how much time the process takes.



With each step, there's a delay as the software is downloaded. This delay is multiplied by the number of devices, and the number of signatures that need updating. Imagine hundreds of devices, on different versions, and the barrage of error messages for dynamic updates (signature updates) that come along with the update process.

This process is time consuming, labor-intensive, error-prone, and disruptive to the network. The team has better things to do than babysit the update process - a process that is repeated across every single firewall every time an update is required.

Fortunately, there's a better way.

On BackBox

BackBox updates are done through the “single-pane-of-glass” console to all automations that BackBox is managing.

There are two steps to the upgrade:

1. Prepare the automation sequence that completes and tests the upgrade.
2. Run the automation.

Preparing the sequence is a straightforward matter of planning. Using the out-of-the-box automations in the Automation Library, administrators build the update process that meets their requirements by chaining together tasks and pre- and post-task checks, in order to ensure a successful update.

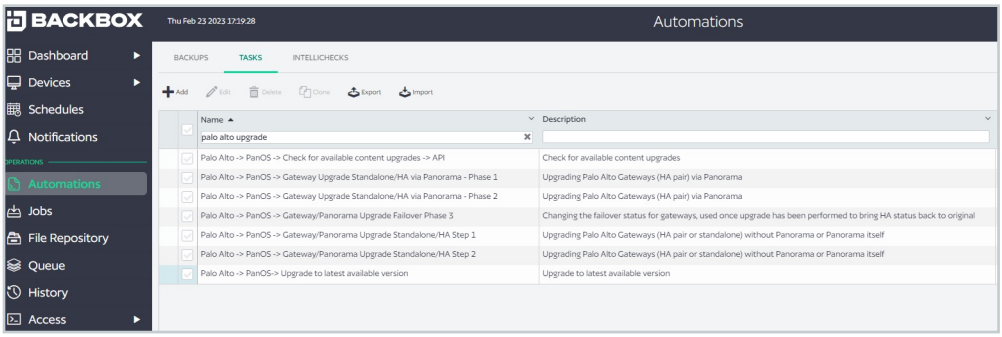


Figure 1: Some of the out-of-the-box automations for Palo Alto

There are only three types of tasks in the Automation Library to chain together for the dynamic signature updates required for Palo Alto:

- Antivirus
- Dynamic (application and threat) signatures
- The update itself

BackBox is also **high-availability aware** and can update the secondary in a cluster after checking that the primary has capacity to take over. And, after updating the secondary, with just a single fail-over, can then update the former-primary.

Here's what that looks like in the BackBox UI:

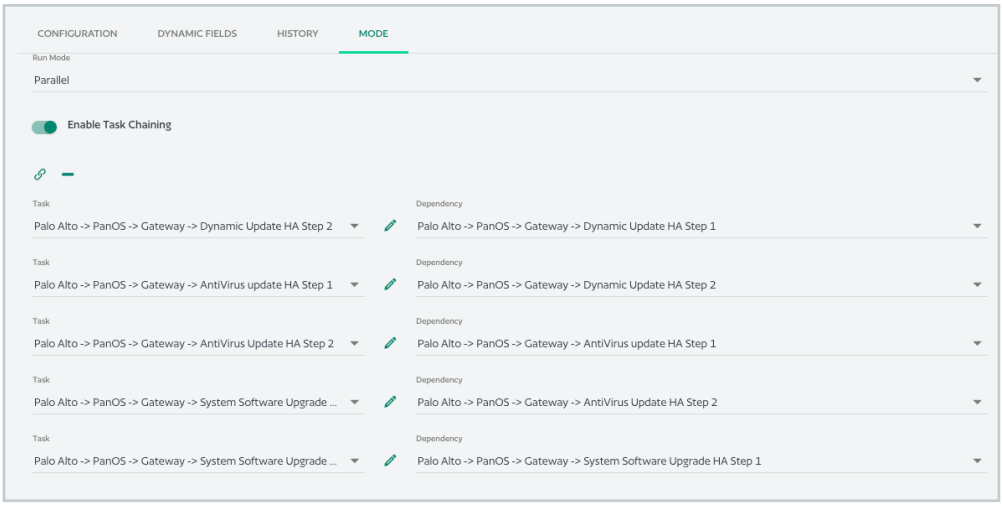


Figure 2: Chaining pre-check automations in BackBox

Automation, Not Just Updates

> Often, administrators think of updates simply as "updating the version of software on my device." In fact, updates are often much more.
>
> **Before an update do you (or are you supposed to) do a backup?**
>
> **Are you supposed to validate that backup to make sure it works?**
>
> **After the update, do you run any tests on the device to make sure the update worked? Do another backup? Do you update a CMDB?**
>
> If the answer to any of those questions is **yes**, then your backup is not simply "update the version of software on my device" but "do some things, update the version of software on my device, then do a few more things".

Let me share a real-world example of a post-check that prevented a upgrade-induced bug from entering production. In this upgrade, SSH v2 was downgraded to v1. The BackBox update post-check automation discovered this change, enabling the administrator to quickly restore to the pre-update backup without any downtime.

That's the difference between executing updates with a vendor tool like Panorama, versus a network automation platform like BackBox.

As part of the larger update process, BackBox completes:

- Any additional pre- and post-checks to make sure the update will work, or did work.
- Validated backups, both before and after. We backup everything needed to restore, so in case something goes wrong, as it often does, with one click you're returning your network to a known working state with all the logs you need to figure out what went wrong. And, since we've checked automatically for signature updates, we know to backup after signatures are updated, so you don't have to redo that work when the time comes to successfully complete the update.
- Updates to a CMDB, or any external system, either with off-the-shelf integration to ServiceNow or via our API.

Of course, the use case in this document is focused solely on updates. Automation can be applied to so many other tasks and desired outcomes that are part of the daily administration of network and security devices (as compared to vendor tools, which only work on their products and have limited automation beyond the specific tasks they're meant to complete).

Conclusion

BackBox eliminates the tedious manual and time-consuming administrative activity that Panorama builds into the update process and enables your team to get more done, in less time, with fewer errors.

BackBox addresses this at scale, and can run pre-checks against the whole network to see where signature updates are needed before starting the update.

BackBox is a network automation platform, so while comparing "update to update," keep in mind that BackBox is much more than a software update tool. Adding automation to your arsenal of administrative tools reduces errors, saves time in many ways, and adds important capabilities like reporting, auditing, and compliance assurance.

About BackBox

Backbox is a Network and Security Device Automation Platform that supports over 180 vendors, with thousands of pre-built automations and a scripting-free way to build new ones. Enterprises and managed service providers worldwide trust BackBox to automate and audit anything an admin could do manually, with reliable automations that are flexible, scalable, and contextually aware. From backups and OS updates to configuration compliance, BackBox gives you confidence that your automations will deliver the expected outcome every time.
Find out more at www.backbox.com