TECHNOLOGY PARTNER PROGRAM

Integration Guide

Author: BackBox Software LTD.

Contents

Partner Information

Partner information	
Date	5/26/2019
Partner Name	BackBox Software LTD
Web Site	www.backbox.com
Product Name	BackBox
Partner Contact	Chanoch Marmorstein, Director of Product Management, chanochm@backbox.com, +972544315214
Support Contact	support@backbox.com
Partner Product for Integration	BackBox
Product Description	Intelligent Automation for Security and Network Devices

Solution Summary

Use cases for integration into the Palo Alto Networks Next Generation Security Operating Platform

- List out use cases for the integration
    - Disaster recovery of Panorama and Palo Alto Networks Firewalls, offering automatic backup and restore of Firewalls
    - Intelligent task automation for Panorama and Palo Alto Networks Firewalls. Few examples:
        1. Automate commit process
        2. Upgrade to the latest available software version
        3. Check for available content upgrades
        4. Set administrative idle-timeout

    - IntelliChecks – Intelligent checks for security, operational and performance compliance that run periodically on Panorama and Palo Alto Networks Firewalls. Few examples:
        1. Stop traffic when LogDB full is enabled
        2. Show throughput and alert on threshold
        3. Strict TCP IP checksum

Palo Alto Networks Products for Integration

P alo Alto Networks Product	Integration Status	Palo Alto Networks versions tested	BackBox versions tested
Aperture			N/A
AutoFocus			N/A

Cortex XDR			N/A
Cortex XDR Analytics			N/A
GlobalProtect			N/A
obalProtect Cloud Service			N/A
MineMeld			N/A
NGFW	FULL	9.0	6.22.02
Panorama	FULL	9.0	6.22.02
RedLock			N/A
Traps			N/A
VM-Series	FULL	9.0	6.22.02
WildFire			N/A
Other			N/A

Integration Benefits

Automated disaster recovery procedures.

BackBox can automate API calls for backup and recovery procedures of Palo Alto Networks products. BackBox has implemented verification methods for the backup files to verify the validity of the files.

Orchestrate and automate daily tasks on Palo Alto Networks Firewalls

With the use of Palo Alto Networks API or CLI connections, BackBox can automate simple to advanced tasks in the customer's network. Some examples are adding rules to policy, doing Firewall batch upgrades while saving time.

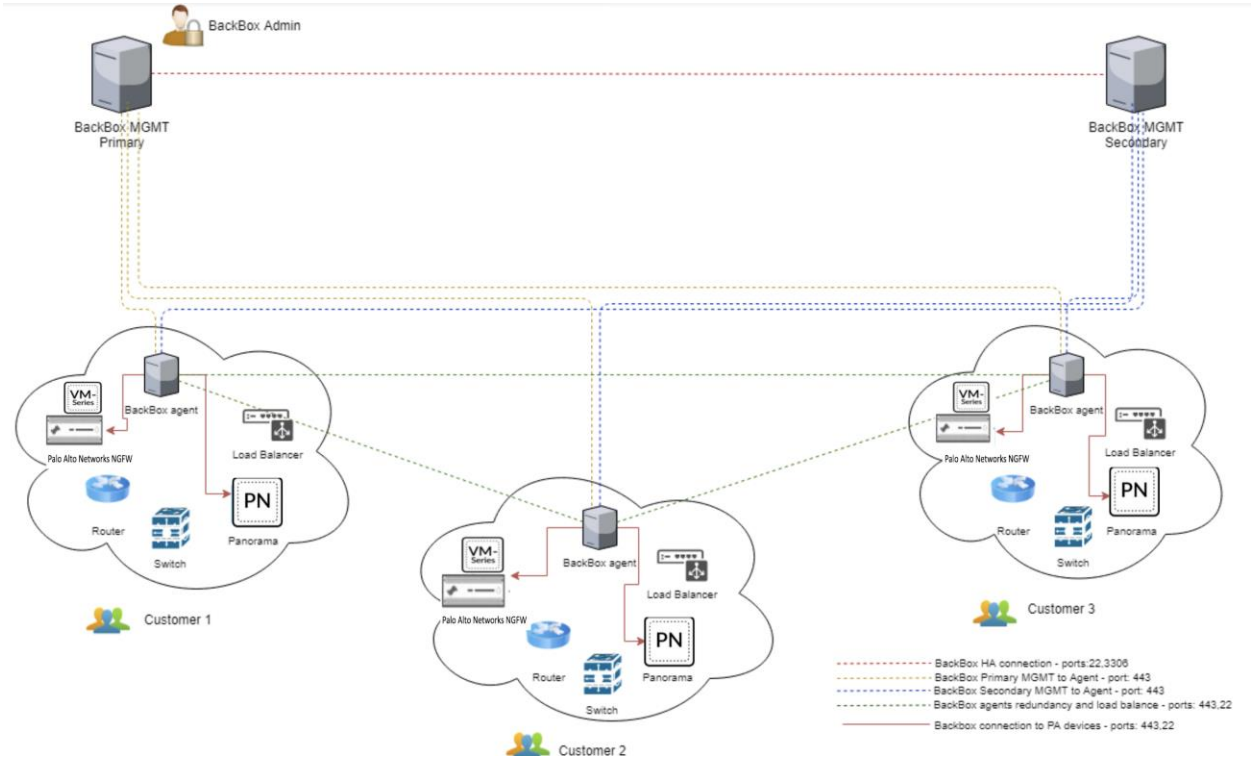
Run periodic checks on Palo Alto Networks Firewalls to prevent the next disaster or downtime

BackBox implemented more than 150 signatures for Palo Alto Networks Firewalls to check for operational compliance, security audits and performance alerts according to Palo Alto Networks best practices.

Dynamic asset management for Palo Alto Networks Firewalls

BackBox is connected to Palo Alto Networks Firewalls and collects software and hardware information during the backup process. This gives the customer a dynamically updated inventory immediately.

Integration Diagram



-
    - *The connection from BackBox to Palo Alto Networks Firewalls is based port 22 and 443 port. BackBox can retrieve any information needed to automate process on Palo Alto Networks Firewalls.*
    - *BackBox can leverage connections through ports 22 and 443 retrieving information from Palo Alto Networks Firewalls or, execute API requests to automate processes and gather information about Palo Alto Networks Firewalls.*

Before you begin

- *BackBox should be configured with administrative credentials to achieve full automation for Palo Alto Networks Firewalls.*
- *BackBox requires ports 22 and 443 open to enable connectivity to Palo Alto Networks Firewalls.*
- *BackBox supports all versions of Palo Alto Networks operating systems, for both Panorama and Palo Alto Networks NGFW.*

Palo Alto Networks Configuration

- *Assure that the Backbox Mgmt Server can connect to the Palo Alto Networks Firewall(s) on the following ports: 443: XML-API and 22: SSH (CLI).*
- *Create a specific Admin role and account for ssh and api access to the Firewall based on best practices.*
  Reference:-
  https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-panorama-api/get-started-with-the-pan-os-xml-api/enable-api-access.html

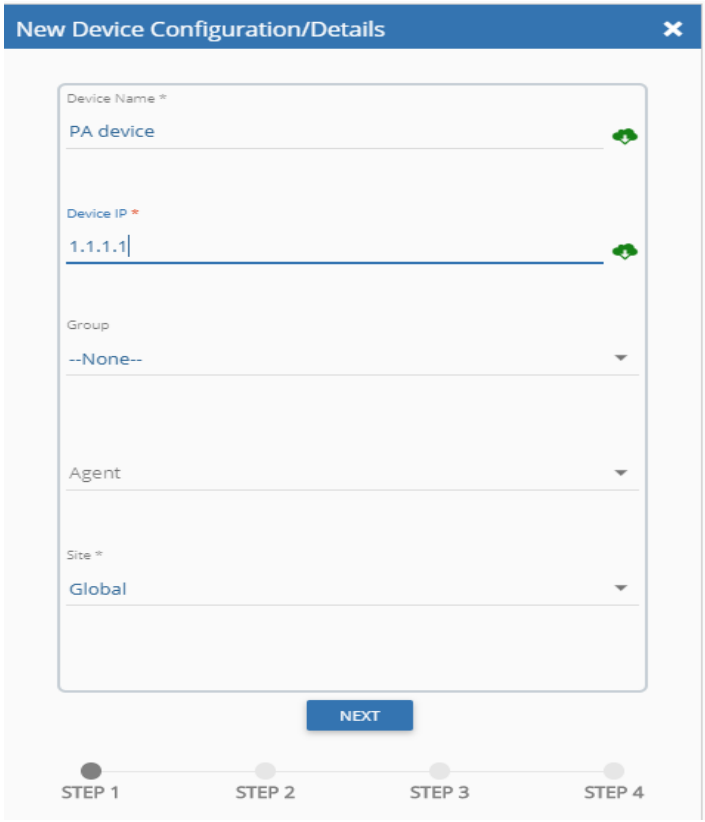
https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/getting-started/best-practices-for-securing-administrative-access.html

Partner Product Configuration

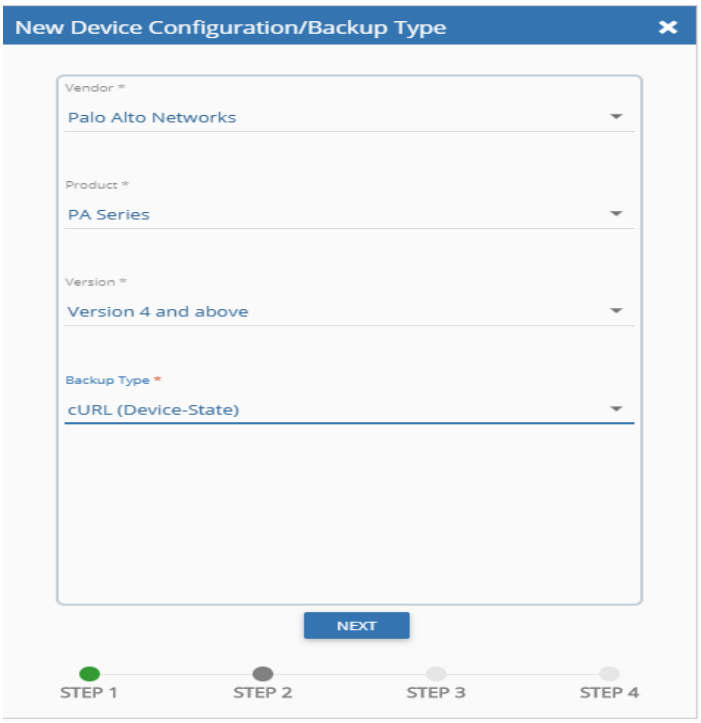
- *Install BackBox on premise in any VM environment or in the cloud.*
- *Configure basic network information within BackBox to connect to your network*
- *Within BackBox, add any Palo Alto Networks Firewall to the Firewall list including administrative credentials*
- *Create backup schedule for Palo Alto Networks Firewalls*
- *Automate Palo Alto Networks tasks within BackBox*
- *Create scheduled IntelliChecks for defined Palo Alto Networks Firewalls*

Steps for adding Palo Alto Networks Firewall on BackBox:

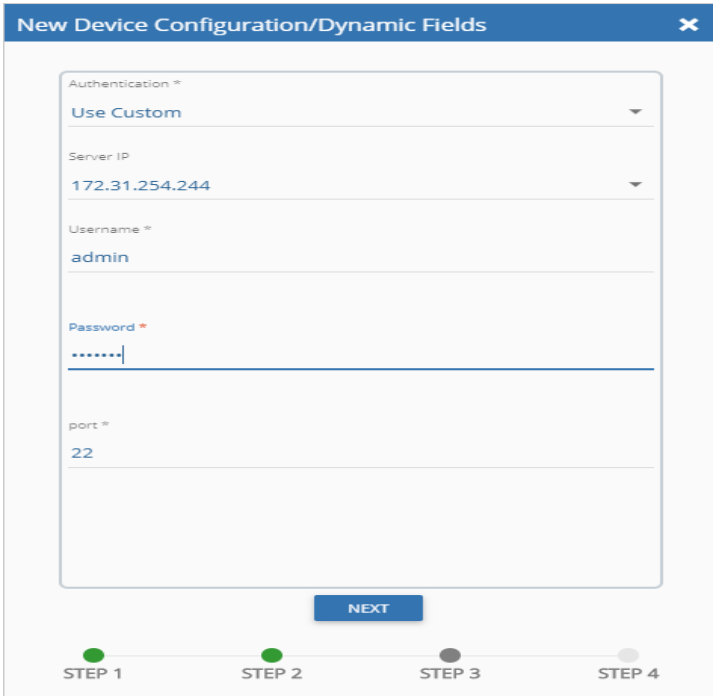
Step 1 – *Firewall name and IP*



Step 2 – *Choose vendor/product/version/option*

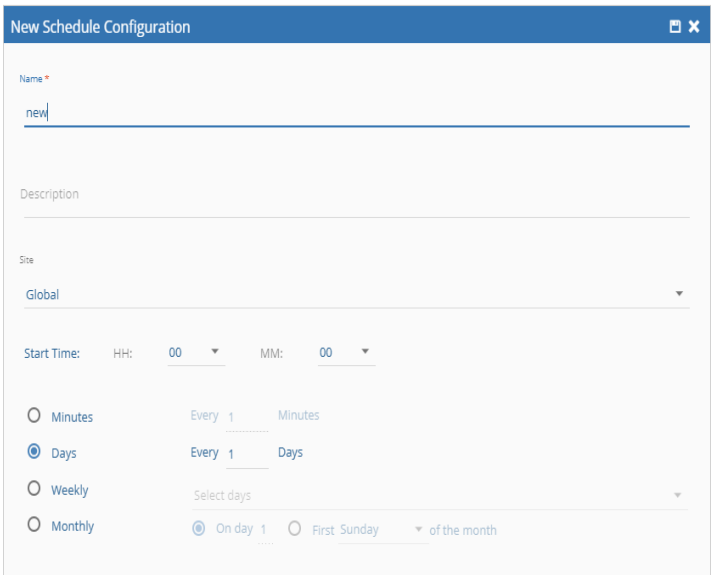


Step3- *Authentication details*

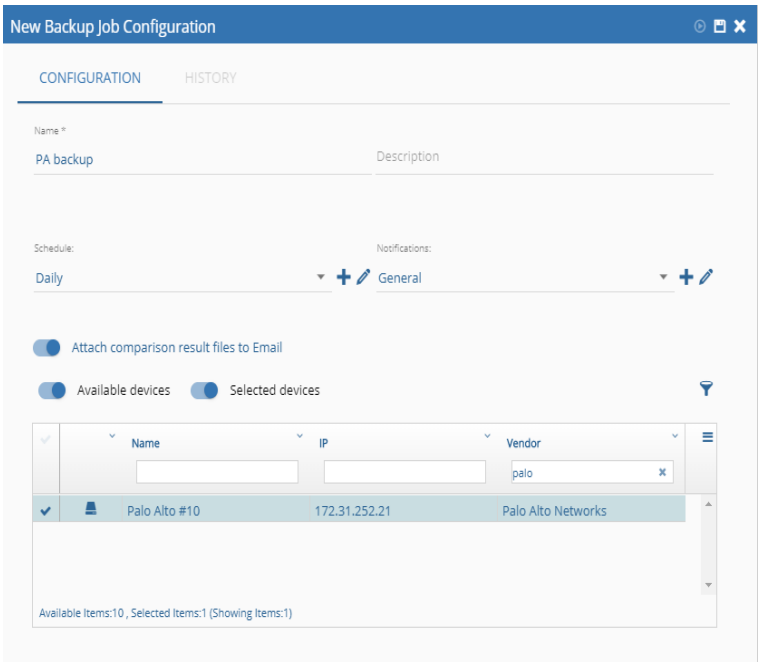


<u>Steps for Creating a Backup Job for Palo Alto Networks Firewall</u>

Step 1 – *Pressing on the + icon near the schedule section will open an option to configure new schedule*

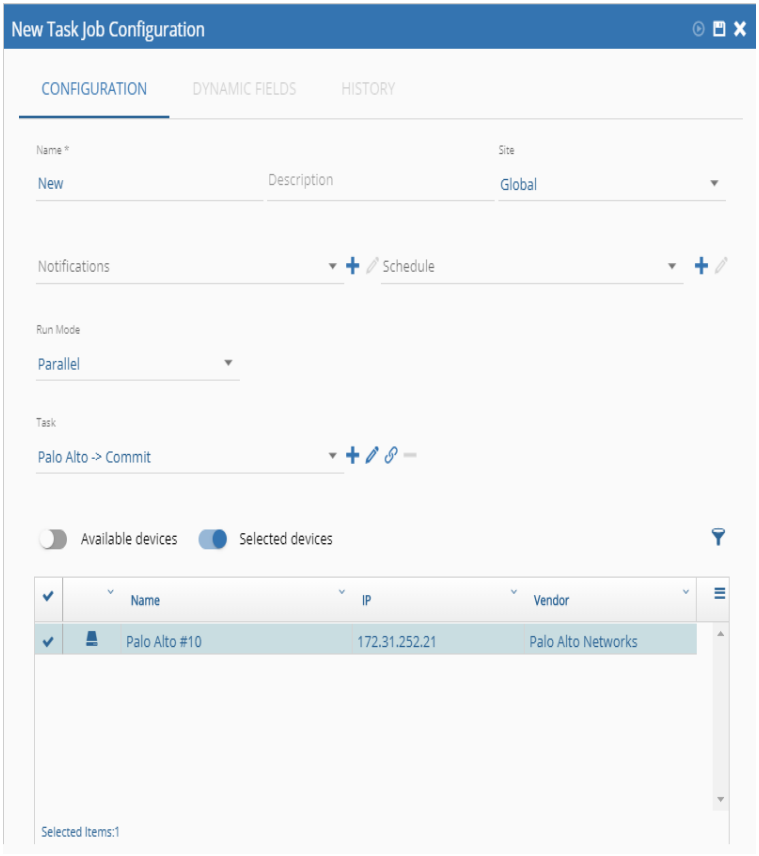


Step 2 – *Create a new Backup Job using the schedule created in step 1.*



Steps for Creating task automation in for Palo Alto devices in BackBox

Step 1 – *Creating a task Job by going to Tasks->Jobs and add a new job*



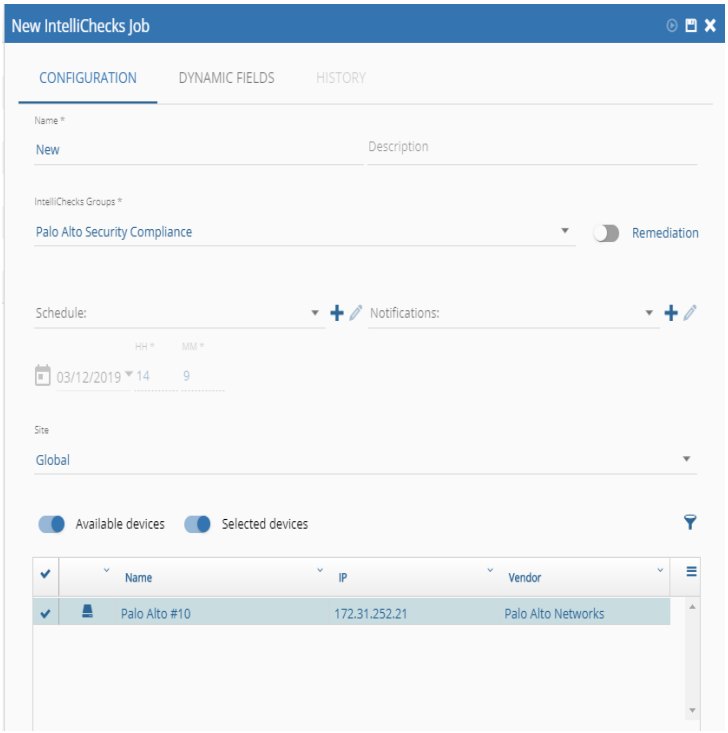
Step 2 – *Select The task to run*

Step 3 – *Select The Devices*

Step 4 – *Select a schedule or run the task immediately*

Steps for Creating Intellicheck jobs for Palo Alto devices in BackBox

Step 1 – *Go into Intellichecks ->Jobs and add a new job*



Step 2 – *Select The Intellichecks group to run*

Step 3 – *Select the devices*

Step 4 – *Select a schedule or run the job immediately*

Troubleshooting

- *Check network connection between Palo Alto Networks Firewalls and BackBox*
- *Check that Palo Alto Networks Firewall credentials are valid*
- *Contact support@backbox.com for any arising issues*
- *Visit www.backbox.com for use cases, support and downloads*

Technical Details

- *Examples for API calls and CLI commands:*
    1. *Config.export API call*
    2. *Show system info CLI command*
    3. *Request License info CLI command*
    4. *Show running config CLI command*
    5. *set firewall config setting management idle-timeout CLI command*
    6. *set rulebase to create new rule CLI command*

7. *Show high-availability state CLI command*
8. *Upgrade PA Firewall to latest version*
9. *Commit changes*
10. *Adding rule to policy*
11. *Check hostname on firewall*
12. *Alert on virtual memory limit*
13. *Verify IPV6 Firewalling*
14. *Verify HA cluster state*
15. *Verify HA cluster configuration sync*
16. *Alert on CPU usage*
17. *Verify SSL decrypt enabled*
18. *Alert on blocked app notification*
19. *Verify NTP sync*
20. *Verify log collector*