BACKBOX

SOLUTION BRIEF

FORTINET

Fortinet and BackBox Integrated Network Security Solution

Centralized Security Solution that Continuously Maintain and Improve Network Security Posture

Integration Highlights

- Automated FortiOS upgrades and patches for all security devices from Fortinet and OS upgrades for devices from other vendors across your network infrastructure in a timely manner to maintain security posture.
- Automated backup of the latest configurations of Fortinet FortiGate NGFWs and other security devices. The self-verification mechanism of BackBox ensures configuration backup files validity.
- Easily restore FortiGate NGFWs configuration with 'single-click' disaster recovery to minimize downtime, even if it is offline and has no connection to the FortiManager.
- Automated remediation of discovered compliance conflicts or security vulnerabilities of FortiGate NGFWs configuration to comply with organization or industry/government policies or standards.
- Monitor device performance and status of FortiGate NGFWs and other network and security devices to predict possible outages so that proactive actions can be taken as preventive measures.
- Automated discovery of FortiGate NGFWs and all other Fortinet devices connected to the network for tight management of device inventory to comply with cybersecurity standards, such as CIS..

The Challenge

As organizations adopt new technologies for digital transformation and the deployment of hybrid and multi-cloud environments to support new applications, their networks are becoming increasingly complex. Manually managing and supporting all network and security devices to ensure business continuity can often be difficult, time-consuming, and prone to error. With cybersecurity threats a continuous source of concern, security devices cannot afford any downtime. Security devices in today's networks also require constant upgrades to maintain the security posture. Failure to backup network and security device configurations can result in significant network downtime and lost business opportunities.

> “The Fortinet and BackBox integrated solution provides automated backup and recovery of FortiGate NGFWs.

The Solution

Today's network infrastructure demands a smart solution that can provide the combined benefits of backup, recovery, and automation for all security devices across the network for unified management. With automated backup of configuration settings and routine performance audits, security settings on all network devices remain secure. And, in case a device on the network does fail, automated backups and timely resolution can significantly shorten recovery time.

BackBox and Fortinet Integrated Solution

The Fortinet and BackBox integrated solution provides automated backup and recovery of FortiGate NGFWs, eliminating the need to either manually backup devices or customize in-house scripting, thus minimizing downtime when recovery is needed. BackBox collects asset information from FortiGate NGFWs and then reports on inventory information, including license information, device model, serial number, and more. BackBox can change operating system-level parameters on multiple devices with a single click, providing customers or network administrators with the option of delegating administrative tasks to individuals who do not require full policy access, in turn minimizing human errors that could lead to configuration errors.

BackBox also provides seamless integration to meet with specific organization and industry standards and requirements. The combined offering of FortiGate NGFW and Backbox is additionally complemented by FortiCare services. Audit services by FortiCare measure operational performance of a firewall in the customer's production environment. Supplemented by personalized reports, it provides a firewall review to identify issues and provide configuration tuning recommendations that create a solid foundation from which to evolve the security infrastructure.

Fortinet Security Fabric ties all of these products and services together to provide enterprises and service providers with a seamless and integrated security posture for their growing and ever-evolving security infrastructure. The Fortinet Security Fabric is designed around a series of open APIs, Open Authentication Technology, and standardized telemetry data to enable organizations to integrate existing security technologies via open interfaces and provide end-to-end security without compromise.

BENEFITS OF THE INTEGRATION:

- Automated, verified FortiOS upgrades of Fortinet devices to maintain network security posture.
- Automated configuration backup for Fortinet devices.
- Single-click disaster recovery and step-by-step disaster recovery procedures.
- Validation and automatic remediation of configurations against policies and regulations.
- Monitor performance and status of Fortinet devices.
- Automated discovery of newly connected Fortinet devices 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.

Fortinet FortiGate NGFWs

FortiGate NGFWs simplify security complexity and provide visibility into applications, users, and networks. Innovative security processor units (SPUs) technology delivers high-performance application layer security services (NGFW, SSL inspection, and threat protection), coupled with the industry's fastest SSL inspection engine to help protect against malware hiding in SSL/TLS encrypted traffic. The platform also leverages global threat intelligence to protect individual customers, by using Fortinet's FortiGuard Security Subscription Services to enable visibility and control for next-generation protection against advanced threats, including zero-day attacks.

Use Case 1

CENTRALIZE AND AUTOMATE FortiOS 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 FortiOS upgrades and patches for Fortinet FortiGate NGFWs and OS upgrades for 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 FortiOS, Fortinet's version of OS security operating system, and upgrade hundreds of devices seamlessly with a single click.

Use Case 2

ENFORCE COMPLIANCE WITH CORPORATE STANDARDS FOR FORTINET FortiGate NGFWs AND ALL 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 Fortinet FortiGate NGFWs and other network security devices for configuration changes and see the deviation with the baseline.

Use Case 3

CENTRALIZE AND AUTOMATE FORTINET FortiGate NGFWs 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:

Seemless integration between BackBox and Fortinet FortiGate NGFWs enables automated, centralized, and secure backups for all configuration information from Fortinet devices. This ensures rapid recovery and minimal downtime.

Use Case 4

MONITOR PERFORMANCE AND STATUS OF FORTINET FortiGate NGFWs 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 and security 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 Fortinet FortiGate NGFWs and all 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.

BACKBOX

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 Fortinet

Fortinet (NASDAQ: FTNT) makes possible a digital world that we can always trust through its mission to protect people, devices, and data everywhere. This is why the world's largest enterprises, service providers, and government organizations choose Fortinet to securely accelerate their digital journey. The Fortinet Security Fabric platform delivers broad, integrated, and automated protections across the entire digital attack surface, securing critical devices, data, applications, and connections from the data center to the cloud to the home office. Ranking #1 in the most security appliances shipped worldwide, more than 595,000 customers trust Fortinet to protect their businesses.

Learn more at www.fortinet.com