

Automate DISA STIGs Compliance with BackBox

Automating compliance saves time while minimizing errors from manual network and firewall administration.

Overview

Federal IT teams within the U.S. Department of Defense (DoD), as well as defense contractors, must comply with testing and hardening frameworks known as STIGs (security technical implementation guides). According to the Defense Information Security Agency (DISA), STIGs **“are the configuration standard for DoD devices and systems, containing technical guidance to lock-down information systems and software that might otherwise be vulnerable to malicious attack.”**

DISA STIG compliance is a measure of whether systems and software are configured to meet standards set by DISA to ensure that systems and networks within the DoD are secure and protected against potential threats. Failure to comply can result in significant fines and heavy scrutiny.

The Challenge

There are three challenges to implementing a compliance regime like DISA STIGs.

- 1. It's Manual.** Device configurations are often validated manually. With over a hundred rules, and potentially multiple vendors manually validating configurations is both time-consuming and error-prone.
- 2. Configuration drift.** It's entirely possible to comply today but not in compliance tomorrow, as device configurations are known to drift off course over time. For agency and program security teams, it often feels like a never-ending catchup to ensure all systems comply.
- 3. Need for reporting.** Auditing compliance is another important dimension of any compliance regime. Automation is the only way to efficiently and effectively audit and report on STIGs compliance.

The Automation Advantage

- Teams can accelerate compliance by creating automation templates that define their compliance requirements and run those templates against groups of devices simultaneously. This eliminates manual work and allows for parallel efforts across many devices.
- Teams can maintain compliance and avoid configuration drift with automated checks against the compliance requirements. Non-compliant devices can be automatically remediated, have audit reports generated, notifications sent, or trouble tickets opened in an ITSM like ServiceNow for manual investigation and remediation.
- Compliance audits are performed regularly, often nightly, without burdening your teams, and compliance reporting can be shared as needed with other parts of the organization.

TIPS FOR CHOOSING A DISA STIGS COMPLIANCE FOR NETWORK CYBER RESILIENCE SOLUTION

There are three things to consider when selecting a solution for automating DISA STIGs compliance:

- 1.** How will the solution perform and scale when automating compliance for hundreds of firewalls or network devices?
- 2.** How easy is it to create any compliance rules needed or to maintain them over time?
- 3.** How quickly can the solution be put into production and begin monitoring compliance?

BackBox and DISA STIG Compliance

The BackBox Cyber Resilience Platform for network infrastructure can help organizations get compliant and stay compliant with the DISA STIGs related to network and security devices.

BackBox is purpose-built to help network teams automate compliance tasks. The platform can help deploy standardized configurations, detect configuration changes, audit configurations, and correct compliance violations. It incorporates a proprietary feed of vulnerability data (including CVEs from the National Vulnerability Database) to help identify and remediate vulnerabilities.

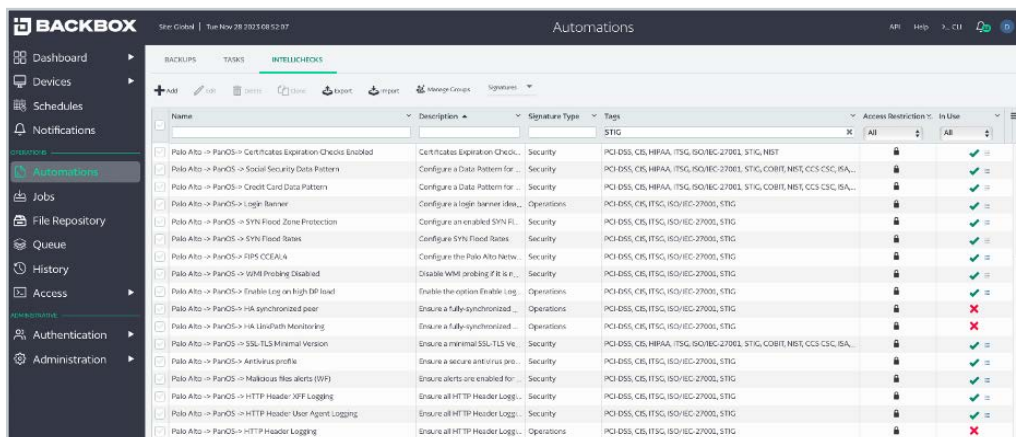
BackBox can also:

- Backup and restore device configurations
- Update device Operating Systems to eliminate vulnerabilities
- Maintain a real-time inventory of network devices and their configurations
- Produce DISA STIGs compliance reports

How to Use BackBox to Automate DISA STIGs Compliance

The first step is to turn the STIG into a set of automations. For example, the BackBox Automation Library already includes 116 pre-built automations that define the STIG for Palo Alto firewalls.

Creating automations for other STIGs is simple. Using the BackBox Automation Builder and only familiar CLI or API commands, automations can be easily created to replicate the work administrators would otherwise do manually.



Name	Description	Signature Type	Tags	Access Restrictions	In Use
Palo Alto -> PaloOS -> Certificates Expiration Checks Enabled	Certificates Expiration Checks...	Security	PCI DSS, CIS, HIPAA, ITSG, ISO/IEC-27001, STIG, NIST	All	✓
Palo Alto -> PaloOS -> Social Security Data Pattern	Configure a Data Pattern for...	Security	PCI DSS, CIS, HIPAA, ITSG, ISO/IEC-27001, STIG, COBIT, NIST, CCS, CSC, ISA...	All	✓
Palo Alto -> PaloOS -> Credit Card Data Pattern	Configure a Data Pattern for...	Security	PCI DSS, CIS, HIPAA, ITSG, ISO/IEC-27001, STIG, COBIT, NIST, CCS, CSC, ISA...	All	✓
Palo Alto -> PaloOS -> Login Banner	Configure a login banner (aka...	Operations	PCI DSS, CIS, ITSG, ISO/IEC-27001, STIG	All	✓
Palo Alto -> PaloOS -> SYN Flood Zone Protection	Configure an enabled SYN FL...	Security	PCI DSS, CIS, ITSG, ISO/IEC-27001, STIG	All	✓
Palo Alto -> PaloOS -> SYN Flood States	Configure SYN Flood States	Security	PCI DSS, CIS, ITSG, ISO/IEC-27001, STIG	All	✓
Palo Alto -> PaloOS -> IPS CCEA/A	Configure the Palo Alto Netw...	Security	PCI DSS, CIS, ITSG, ISO/IEC-27001, STIG	All	✓
Palo Alto -> PaloOS -> IGMP Probing Disabled	Disable WMI probing if it is...	Security	PCI DSS, CIS, ITSG, ISO/IEC-27001, STIG	All	✓
Palo Alto -> PaloOS -> Enable Log on high IP load	Enable the option Enable Log...	Operations	PCI DSS, CIS, ITSG, ISO/IEC-27001, STIG	All	✓
Palo Alto -> PaloOS -> HA synchronized peer	Ensure a fully-synchronized...	Operations	PCI DSS, CIS, ITSG, ISO/IEC-27001, STIG	All	✗
Palo Alto -> PaloOS -> HA Link/With Monitoring	Ensure a fully-synchronized...	Operations	PCI DSS, CIS, ITSG, ISO/IEC-27001, STIG	All	✗
Palo Alto -> PaloOS -> SSL/TLS Minimal Version	Ensure a minimal SSL/TLS Ve...	Security	PCI DSS, CIS, HIPAA, ITSG, ISO/IEC-27001, STIG, COBIT, NIST, CCS, CSC, ISA...	All	✓
Palo Alto -> PaloOS -> Antivirus profile	Ensure a secure antivirus pro...	Security	PCI DSS, CIS, ITSG, ISO/IEC-27001, STIG	All	✓
Palo Alto -> PaloOS -> Malicious file alerts (WFP)	Ensure alerts are enabled for...	Security	PCI DSS, CIS, ITSG, ISO/IEC-27001, STIG	All	✓
Palo Alto -> PaloOS -> HTTP Header: XFF Logging	Ensure all HTTP Header Logg...	Security	PCI DSS, CIS, ITSG, ISO/IEC-27001, STIG	All	✓
Palo Alto -> PaloOS -> HTTP Header: User Agent Logging	Ensure all HTTP Header Logg...	Security	PCI DSS, CIS, ITSG, ISO/IEC-27001, STIG	All	✓
Palo Alto -> PaloOS -> HTTP Header Logging	Ensure all HTTP Header Logg...	Operations	PCI DSS, CIS, ITSG, ISO/IEC-27001, STIG	All	✗

The BackBox automation team can also help write additional automations to get customers up and running quickly.

After each STIG has been implemented as a set of automations within BackBox, it is then applied to a specific set of devices and run on a regular schedule. When the STIGs automations are run, devices are checked against the compliance rules. If found to be out of compliance, three steps can be taken:

1. The device can be automatically remediated,
2. A report can be created and a notification sent to appropriate teams to investigate, or
3. BackBox can automatically open a trouble ticket with details of the compliance failures.

For one customer, BackBox reduced the number of manual steps from 92 to a single set of automations that automatically run each day across hundreds of Palo Alto firewalls. Eliminating the need for daily manual processes resulted in fewer errors and more regular compliance testing.

Conclusion

Vulnerability DISA STIGs compliance, while primarily designed for DoD organizations and related defense contractors, is yet another framework for building best-practice security into network and firewall device configurations.

Manually enforcing DISA STIGs, however, is both error-prone and lacks the scale necessary for realistic day-to-day management of network devices. Automation is the answer. Automation eliminates errors from manual device configuration activities while at the same time automatically ensuring that devices remain compliant and simplifying audit and reporting.



About BackBox

More than 500 enterprises worldwide trust BackBox as their preferred network cyber resilience platform. BackBox supports network devices from over 180 vendors, offering thousands of pre-built automations and a no-code way to create new ones. BackBox empowers teams with the confidence to automate critical network processes, maintain business continuity during disruptions, and recover swiftly. From backups and OS updates to configuration compliance and vulnerability management, BackBox ensures that automations deliver consistent, reliable outcomes.

To learn more, visit backbox.com