Your security policies are designed to ensure your organization keeps bad actors out of your network — while still meeting regulatory requirements. But the ever-changing needs of your business mean your network continually changes as well. Typically, maintaining continuous compliance in this complex, hybrid network means labor-intensive, non-stop attention.

Skybox® Security’s automated approach to policy compliance reduces your risk of breaches and regulatory costs while simplifying management to maximize your team’s efficiency.

A key benefit to using Skybox for policy compliance management, especially in hybrid environments, is its centralization. Skybox serves as your go-to solution to compare the reality of your hybrid network against your many policies. Whether you’re working with on-prem network devices or public or private cloud infrastructures, Skybox can determine if the aggregate access is exceeding what’s designed in policy. It also provides you not only the means to achieve compliance, but to maintain continuous compliance with intelligent, automated change workflows.

Skybox helps support a wide range of industry- and region-specific compliance standards including PCI DSS, NERC, NIST, FISMA, HIPAA, SOX and GDPR, among others. But no matter the regulation you’re subject to, Skybox helps you follow the ultimate best practice: the principle of least privilege. With Skybox, you can ensure access is limited to only what’s necessary, keeping you in compliance with the rainbow of regulatory mandates — and keeping bad actors out of your network.
Skybox defines the compliance of network infrastructure by three distinct engines:

- **Configuration Compliance**: Audit the platform security of devices to identify configuration weaknesses; assess whether the device can be accessed using the default password, if logging is enabled and if the management protocol is encrypted.

- **Rule Compliance**: Verify whether the access rules of a device meet specific criteria as well as widely accepted industry best practices for network device operations.

- **Access Compliance**: Formalize the access-related standards you want to enforce in your network.

**Configuration Compliance**

Too often overlooked, configuration compliance is key to limiting your risk of attack. Meeting other compliance requirements (such as in rule and access compliance) does little good if the devices ensuring your security aren't properly configured. Misconfigurations are an all-too-common attack vector undermining what could otherwise be a strong security program.

Skybox provides numerous platform-specific configuration policies which can be adopted as-is or customized to suit your business needs. Policies contain a set of configuration checks, each of which is represented by regular expression. When a device's configuration data is analyzed, it passes only if the regular expression is matched in the configuration file.

Several sources are used for this type of audit including DISA STIGs and CIS Benchmarks. Skybox also uses vendor-specific guidance and best practices for the operational of specific device versions.

**Rule Compliance**

The Skybox rule compliance feature ensures rules are written according to the principle of least privilege, using automated analysis to find overly permissive rules.

Skybox’s rule policy engine compares a device’s access rules (where applicable) with one or more rule policies as appropriate. Individual rule policies contain syntactic rule checks which include basic standards for access rules.

Skybox comes with comprehensive, out-of-the-box rule policies that are applied to all devices with access rules by default; customized policies can be created as well. Users can exclude selected devices from specific syntactic checks and/or policies as required.
FIG 2: The rulebase compliance view provides at–a–glance insight to the compliance status of the firewall, the breakdown of violations by severity and details of those violations.

Access Compliance

Ensuring network devices are properly enforcing policy is a challenge even within traditional, on-prem networks. Add the complexity of public and private clouds and microsegmentation, and the task becomes impossible by manual means. But because of Skybox’s knowledge of the network routing, organizations can set policy and see how it’s being enforced in reality on an ongoing basis.

FIG 3: The access policies view provides quick insight to violations between a source or sources and a destination, the criticality of the violation, among other details.
About Skybox Security

Skybox provides the industry’s broadest cybersecurity management platform to address security challenges within large, complex networks. By integrating with 130 networking and security technologies, the Skybox® Security Suite gives comprehensive attack surface visibility and the context needed for informed action. Our analytics, automation and intelligence improve the efficiency and performance of security operations in vulnerability and threat management and firewall and security policy management for the world’s largest organizations.

www.skyboxsecurity.com  |  info@skyboxsecurity.com  |  +1 408 441 8060

Copyright © 2019 Skybox Security, Inc. All rights reserved. Skybox is a trademark of Skybox Security, Inc. All other registered or unregistered trademarks are the sole property of their respective owners. 07032019

The Skybox approach ensures data centers aren’t exposed to the internet on SMB ports and ensures compliance with standards such as PCI DSS and NIST. Zones are created to represent one or more networks, including public networks outside of the organization, trusted network within the organization, a DMZ and any partner/third-party connections. Access between these zones is defined as a white or black list of ports and applications.

Access policies are fully customizable to meet the specific needs of your organization.

Stay Ahead of the Compliance Curve

While networking equipment facilitates the connection of business systems to assist business efficiency, network security devices reduce risk and exposure by restricting traffic flows to only allow business required traffic whilst denying all other.

Skybox provides you with a streamlined mechanism for keeping your devices running to meet business-critical requirements while reducing unnecessary exposure and risk.

To learn more, please visit the links below:

• Network Assurance Datasheet
• Firewall Assurance Datasheet
• Change Manager Datasheet

“Firewall rule changes have guidelines that could fill a book. By automating this process and customizing Skybox to incorporate our various and unique policies, if there’s any violation during a rule change, we know immediately.”

- Associate Director, Business and Technology Services Provider