



SKYBOX SECURITY AND ZSCALER

INTEGRATION FOR FIREWALL AND SECURITY POLICY MANAGEMENT

Technology Brief

Security policies are only as good as the security controls that enforce them. To ensure your Zscaler Cloud Firewall is maintaining compliance with internal policies, region- and industry-specific regulations, and best practices, you need to continually test that the access allowed in your network doesn't exceed what's designed in policy. And, to enable your business, you need to ensure desired access is granted securely.

To support these compliance, security and business objectives, Skybox Security has integrated with the Zscaler Cloud Security Platform. The integration gives customers with Zscaler Cloud Firewall a way to ensure they're adhering to policies and automatically flag violations to address them quickly.

- Confirm Zscaler security controls are enforcing desired enterprise-wide access policies
- Analyze network paths containing Zscaler Cloud Firewall end to end — between and within networks — to ensure proper connectivity and segmentation
- Ensure Zscaler rules are created according to enterprise best practices and identify overly permissive rules
- Visualize Zscaler Cloud Firewall in relation to your hybrid network topology, other security controls, assets and vulnerabilities



How it Works

Skybox collects all the relevant information from the Zscaler Cloud Security Platform and builds it into the Skybox model that includes the hybrid network topology, other security controls, assets and vulnerabilities.

Zscaler local internet breakouts are easily visualized within the Skybox network model, from the edge router outward to the Zscaler Cloud Firewall and Platform.

With the collected Zscaler Cloud Firewall data and model, the Skybox® Firewall Assurance and Skybox® Network Assurance modules can support the following use cases:

- **Access analysis:** simulate access end to end — between and within networks including on-prem, virtual, public and private cloud and operational technology (OT) environments — to ensure proper connectivity and segmentation is in place
- **Rulebase compliance:** ensure security controls continuously maintain compliance with defined access and rule policy by regularly automating assessment of your network's aggregate access
- **Rule review:** automate the review process of existing firewall rules to keep Zscaler Cloud Firewall clean and optimized, limit the lifespan of risky rules and flag violating rules for early review; each rule is assigned an owner, a review date and other metadata to maintain the automated system
- **Network map:** automatically collect and build Zscaler Cloud Firewall data into a visual and interactive network map to have continuous visibility of your hybrid environment and its accessibility
- **Change tracking:** keep track of all Zscaler Cloud Firewall rule changes for compliance or rule review analysis

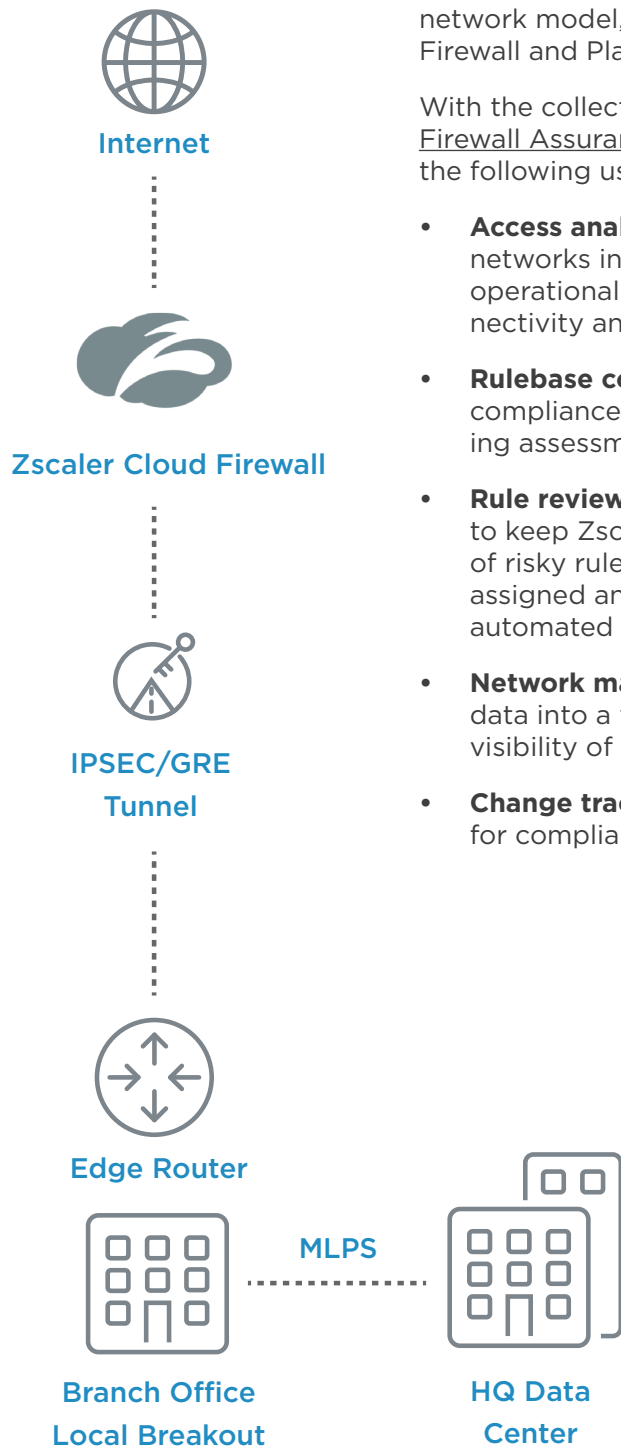


FIG 1: A representation of the Zscaler Cloud Firewall within the Skybox model as it relates to the internet, VPN/GRE tunnel to the on-prem firewall and beyond

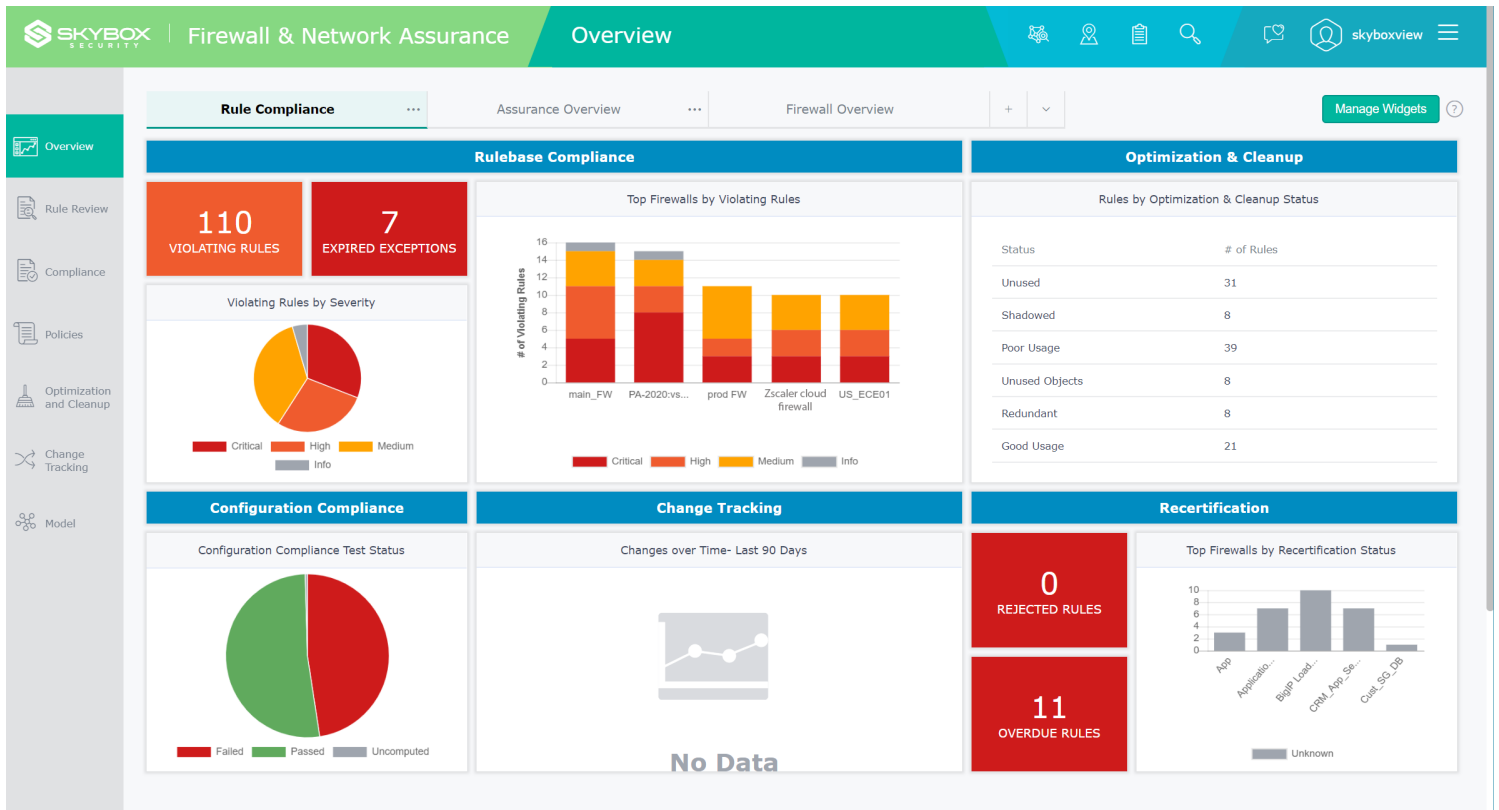


FIG 2: The overview dashboard of the Skybox Firewall and Network Assurance interface, providing a normalized view of rule and configuration compliance, optimization and cleanup status and rules awaiting recertification review.

SKYBOX VALUE

- Unifies security policy management across hybrid networks and multi-vendor environments
- Ensures security controls enable reliable connectivity and maintain continuous compliance
- Automatically identifies rule, access and configuration compliance violations
- Automates and simplifies auditing and reporting

ZSCALER VALUE

- Provides security and access controls for internet traffic on all ports
- Provides identical protection no matter where users connect — policies are not tied to a physical location
- Scales elastically to natively inspect SSL encrypted traffic and delivers integrated next generation firewall, sandboxing, data loss prevention, and CASB capabilities
- Logs every session to give visibility into all users, locations, applications, ports and protocols, in near-real-time



To learn more about the benefits and use cases around Skybox-Zscaler integration, [visit our website](#) or [schedule a demo](#) today.

Related Resources

From Skybox

- [Smart Automation for Security Policy, Firewall and Change Management](#)
- [Firewall Optimization and Cleanup Solution Brief](#)
- [Skybox Firewall Assurance Datasheet](#)
- [Skybox Network Assurance Datasheet](#)

From Zscaler

- [Zscaler Cloud Firewall eBook](#)
- [Transform How You Deliver Internet and Web Security eBook](#)

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

About Zscaler

Zscaler enables organizations to securely transform their networks and applications for a mobile and cloud-first world. Zscaler cloud-delivered services securely connect users to their applications and cloud services, regardless of device, location, or network, while providing comprehensive threat prevention and a fast user experience. All without costly, complex gateway appliances.

www.zscaler.com