Structured workflows are intended to improve the speed, accuracy and security of firewall rule and object changes. But often the benefits of change management processes are undercut by complexity, lack of insight and limited resources.

Details make or break the change workflow. Without the proper information around the change request; visibility of the affected firewalls and network paths; and knowledge of the relevant policies and vulnerability risks, a simple change could nullify a whole layer of security. The chance of security issues and other errors only increases with manual processes. To make sense of all of these details and act on them quickly requires intelligent automation.

Skybox Security’s automated change workflow helps to speed up the firewall rule and object creation process — without sacrificing security. With context-aware planning and risk assessment, Skybox reduces the chance of risky changes going into production, meaning fewer rollbacks and less time spent on rework. The workflow is also customizable to ensure it fits the needs of your organization, its teams and its technologies.

- Harness analytics-driven automation to speed up changes, reduce risk and avoid rollbacks
- Proactively assess policy violations and vulnerability exposures before changes go live
- Customize and standardize automated workflows to fit your organizational needs
Secure Change Workflow

Like all modules of the Skybox® Security Suite, Skybox® Change Manager is powered by an advanced analytics engine. It leverages comprehensive network modeling and path analysis to automatically identify all devices relevant to the change, and to check if the proposed change is already in effect. It then assesses the change request against applicable security policies to avoid regulatory violations and maintain internal security standards.

Skybox also includes the important phase of risk assessment in the change workflow. Because of its insight to the asset layer as well as network topology, Skybox can identify changes that would open up a potential attack path to a vulnerable asset. All this analysis and assessment is done automatically and before the change goes live, giving operations teams a chance to address discovered security and compliance concerns or request the change be amended. Approved changes can be provisioned automatically.

Last but not least, Skybox provides third-party validation to ensure changes match the original request and were implemented as intended.

BUSINESS BENEFITS OF INTELLIGENTLY AUTOMATED CHANGE WORKFLOWS:

- More than 80 percent* reduction in firewall management time
- Cost savings of more than USD$400,000* in the first year, compared to manual change management costs

*Based on actual data from a 150-firewall deployment with 100 changes per firewall per year

Request
User requests desired access via ticketing system

Identify
Identify relevant firewalls and check existing access

Assess Compliance
Identify potential security policy or regulatory compliance violations

Assess Risk
Spot vulnerable asset exposures

Provision
Formalize rule and object changes and choose to push changes live

Verify
Ensure the final change matches the original intent
Ticketing System Options

Change Manager’s workflow phases are driven by a ticketing system, either used for the entire change process, or through an integration with an existing service management ticketing systems such as ServiceNow or Remedy.

For these third-party integrations, there are two main integration models:

- **Bi-Directional Integration**: Users interact with both the Change Manager and the third-party ticketing system’s user interfaces, with both solutions sharing information through their respective APIs.

- **Shadow Ticketing**: Skybox serves as the back-end analytics engine to a third-party ticketing system via the Skybox API; users interact only with the interface of the third-party ticketing system, not Change Manager.

**FIG 1**: Skybox Change Manager let’s you customize and standardize workflows for your entire organization or set unique workflows for different regions, business groups, etc. The left-hand menu also gives you quick access to ensure tickets are progressing quickly with proper oversight.
Don’t let rule and object creation bog down your business’ agility or put security at risk. Leverage network-aware planning and risk assessment that keeps your network secure and in continuous compliance with policies. And reduce resource drain with intelligent automation, customization and integration with your existing technology.

- Fully automate firewall change management workflows, improving communication and efficiency across security teams
- Validate proposed firewall changes by checking for policy violations, security gaps and vulnerabilities that could be exposed by the change
- Ensures that changes are made as intended and do not introduce new risk
- Customize and simplify workflows to reduce change management time by 80 percent

To learn more about Skybox Change Manager, schedule a demo or see the role change management plays in the full set of Skybox solutions for firewall and security policy management.