



Firewall Change Management

Improve IT Efficiency by Automating Firewall Change
Workflow Processes

Executive Summary

Firewall management has become a hot topic among network and firewall professionals, particularly for enterprise organizations. Firewall configuration and maintenance processes that are fairly simple and straightforward when managing a few firewalls can be incredibly time consuming when there are tens or hundreds of firewalls deployed. The struggle to keep firewalls configured properly can severely impact network availability, access, security, and compliance with regulations, not to mention reduced IT productivity and added management costs.

For enterprise IT organizations, having an effective firewall change control process is key. A typical organization may need to make firewall changes hundreds of times in a month, with each change requiring hours of evaluation time to assess potential impact to business continuity and security. A flaw in the way a change is performed might block the access to critical services, or significantly increase the level of exposure to threats, or break firewall compliance with regulations.

Surprisingly, most organizations lack an integrated and automated workflow approach for this critical process. Disconnected, manual process steps and handoffs lead to poor communication and impair tracking. Separate databases of network and firewall-related information make it difficult for a network analyst to evaluate security and availability risks. Workflow tools and process automation have a significant impact on IT productivity and firewall change accuracy — linking the steps, communications, supporting data, and handoff mechanisms needed to have a successful change process.

This white paper presents the current challenges in managing firewall changes, the typical firewall change management cycle, and the concepts of an automated workflow system that address these challenges. Finally, this paper will discuss the unique characteristics of Skybox Change Manager and its ability to automate and streamline the change management process.

Introduction

The dynamic nature of computer networks makes day-to-day firewall management very challenging. To keep up with new users, new business services, and new technologies, computer network environments change frequently. Often, these changes have an impact on the configurations of firewalls. New applications are introduced or a group of users are added to a service, requiring a change to access rules. Applications are extended to include more servers or to communicate with other applications, affecting firewall configuration settings. Major network topology changes may be made to support new networking requirements or to mitigate the risk of a new type of security threat — requiring a complete evaluation of firewall configurations and rules.

Firewalls limit or provide access to network segments depending on a set of firewall rules. To handle the complex access decisions for a typical enterprise network, each firewall may contain hundreds or thousands of rules that specify how and where certain types of traffic can flow. These decisions may be based on security or access policies, application needs, type of request, and more.

IT Standards Recommend Formal Change Management Processes

To reduce the likelihood of change-driven risks to IT security, compliance, and network availability, many IT standards recommend that IT organizations put in place a set of administrative controls around change management processes, such as:

- Establishing a documented change management process
- Change impact analysis prior to every change, including assessment, prioritization, and authorization
- Change tracking and reporting to ensure proper changes have been made as planned and authorized

For example, the following excerpt from the COBIT IT Controls Framework recommends implementing a formal change management process to assess impacts, authorize, define, document, and track IT changes.

A16Acquire and Implement
Manage Changes

CONTROL OBJECTIVES

AI6 Manage Changes

AI6.1 Change Standards and Procedures
Set up formal change management procedures to handle in a standardised manner all requests (including maintenance and patches) for changes to applications, procedures, processes, system and service parameters, and the underlying platforms.

AI6.2 Impact Assessment, Prioritisation and Authorisation
Assess all requests for change in a structured way to determine the impact on the operational system and its functionality. Ensure that changes are categorised, prioritised and authorised.

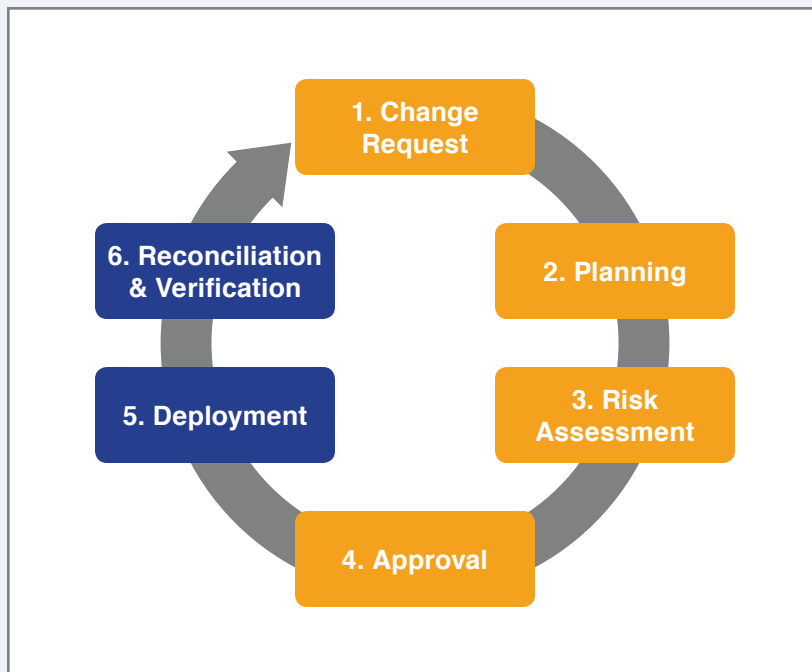
AI6.3 Emergency Changes
Establish a process for defining, raising, testing, documenting, assessing and authorising emergency changes that do not follow the established change process.

AI6.4 Change Status Tracking and Reporting
Establish a tracking and reporting system to document rejected changes, communicate the status of approved and in-process changes, and complete changes. Make certain that approved changes are implemented as planned.

Figure 1 – COBIT IT Controls

Strong change management practices are part of the underpinnings of many IT best practice standards. COBIT, ITIL, NIST, ISO, FISMA, PCI DSS, and a host of other IT frameworks contain lifecycle definitions and recommendations to institute quality change management within IT organizations.

A Typical Firewall Change Management Cycle



Let us consider how a recommended change management lifecycle applies specifically to firewall changes. The diagram to the left illustrates the pre-deployment phases 1 – 4 (orange) from the time the change request is initiated to approval of the change. Post-deployment phases 5 – 6 (blue) cover implementation of the change and verification that the change has been completed and results affirmed.

Figure 2 – A Typical Change Management Cycle

Phase	Behavior
Change request is issued	<ul style="list-style-type: none"> Typically by IT or business owner The request is usually specified in network terms (example: access is needed from source A to destination B using port X), and may or may not relate to a specific firewall
Plan the details of the change	<ul style="list-style-type: none"> A network or firewall expert identifies the firewalls which should support the requested connectivity and addresses the change request Implementation details might be added to the request at this phase or later (e.g. rules or objects to be added or changed)
Assess the potential risk exposure	<ul style="list-style-type: none"> Each planned change request is evaluated to assess its risk, compliance, and business justification People from different disciplines might be involved in the process (dependent on risk) The depth and formality of the process differs from organization to organization <p>Note: An initial assessment may be held even before planning, based on the end-to-end access requests</p>
Approval	<ul style="list-style-type: none"> The request may be approved, rejected, or approved with modifications based on the assessment results
Deploy the change	<ul style="list-style-type: none"> Changes to the firewall rule base are implemented (ACL rules, NAT rules and objects)
Reconcile and verify	<ul style="list-style-type: none"> Changes to firewall configuration are identified (change tracking) Identified changes and approved change requests are compared It is verified that the identified changes correspond directly with approved requests and requests are implemented as specified. Deviations are highlighted. The verified change requests are closed

Current Challenges in Managing Firewall Changes

Most IT organizations today have implemented a firewall change management process that covers some or all of the recommended stages, but usually in a highly manual approach that has been pieced together to try to connect various IT teams, tools, policies, and priorities.

Making a firewall change typically requires different teams in network operations and IT security — groups that may use different tools and information. Ensuring that the streams of change requests from all parts of the organization will be addressed consistently, on time and in a safe way is a major challenge for enterprise IT organizations.

Fragmented Change Processes are Highly Inefficient

Forrester estimates that 80% of the typical IT operations budget is wasted due to inefficiencies (Reference # 1). Integrating firewall change control processes and tools can significantly reduce the amount of time spent on repetitive and inefficient IT tasks, accomplishing a number of objectives:

Linking firewall change workflow tasks together in a common framework accomplishes a number of objectives:

First, it gives the IT and network groups a centralized environment to communicate firewall change information between team members. Instead of multiple tickets, emails, sticky notes, and Excel files, one common process links the planning, evaluating and verification steps.

Second, it provides the structure to capture the details of a proper firewall change request in a consistent way. As part of the workflow mechanism, tools specifically built for firewall change management may also include aids to assess risks.

Finally, integrating the firewall change workflow creates a closed-loop process. Changes and handoffs can be tracked and verified in a systematic way that supports audit needs, providing improved security and compliance with policies. It also helps avoid communication headaches and team infighting, while eliminating emergency rework.

When the steps in a change control process and supporting tools are fragmented, it takes an enterprise network and operations teams an exorbitant amount of time and energy to communicate firewall change requests, evaluate changes, and link actual changes back to the desired outcome.

Disparate Data Repositories Can Camouflage Risk Exposures

Disparate databases, formats and descriptors add to the complexity of comparing and correlating firewall information through the change lifecycle. For example, to accurately describe a firewall change, the IT team may need to compare data from multiple types of firewalls with varying configuration settings and rule formats. To assess the risk of a change, multiple IT members may need to correlate change requests against the configuration management database, the policy repository, and other known risk factors.

Normalized data in common or integrated repositories makes it significantly easier to find potential risk exposures, such as security gaps that can be introduced by the change, compliance violations, or access and availability issues. Common data formats or links between types of data can help give business, operations, and security managers a consistent view into the change process and lessen the chance of errors.

Multiple databases also increase the cost and time required for change verification and reconciliation. Tracking the effect of actual changes across multiple data repositories requires considerable manual correlation and review time. This also increases the likelihood of a late discovery of an error or risk exposure.

When firewall rules, configuration data, corporate access policies, industry standards and the like are stored in separate repositories that do not communicate, IT teams can easily overlook potential threats or access issues that happen through the combination of different factors.

Manual Analysis Can Not Keep Up with Change Process

The change planning and design stage is the first place where manual analysis may significantly slow down the process. A change request may impact several firewalls and understanding which of these firewalls need to be changed is a non-trivial task. Furthermore, deciding how to implement a required change on an existing firewall with hundreds or thousands rules is time consuming.

Manual evaluation of a firewall change request will likely increase the chance of a risk exposure and re-work after the change is implemented because organizations may conduct only a shallow risk assessment due to resource constraints.

Automated analysis helps with the time-consuming and repetitive steps of correlating data and analyzing multiple firewalls. Best-practice checks can be conducted based on the type of change requested or the corporate policy, improving the quality of the assessment steps. As a result, evaluators can start with consistent high-quality assessments, so they can better identify if the requested change:

- Imposes any significant security risk
- Violates compliance with guidelines and regulations (e.g., PCI-DSS)
- Is likely to cause any performance degradation or network downtime

When an organization has a complex network, the manual effort required to describe a firewall change, evaluate the risk of a change, and reconcile change requests is difficult and requires special expertise. Change requests pile up awaiting scarce IT security resources, or short-cuts may be taken to avoid creating an IT bottleneck.

Automated System for Firewall Change Management

To address these challenges organizations must adopt an efficient and effective change management process that integrates all steps in the change workflow, and automates each step as much as possible to relieve the burden on network operation and IT security.

While in the past organizations typically developed in-house solutions, or tailored generic workflow systems to their needs, there are now automated change management systems to support integrated processes, provide a common data repository, and automate analysis to improve the accuracy and speed of the firewall change process.

The Components of an Automated Firewall Change System

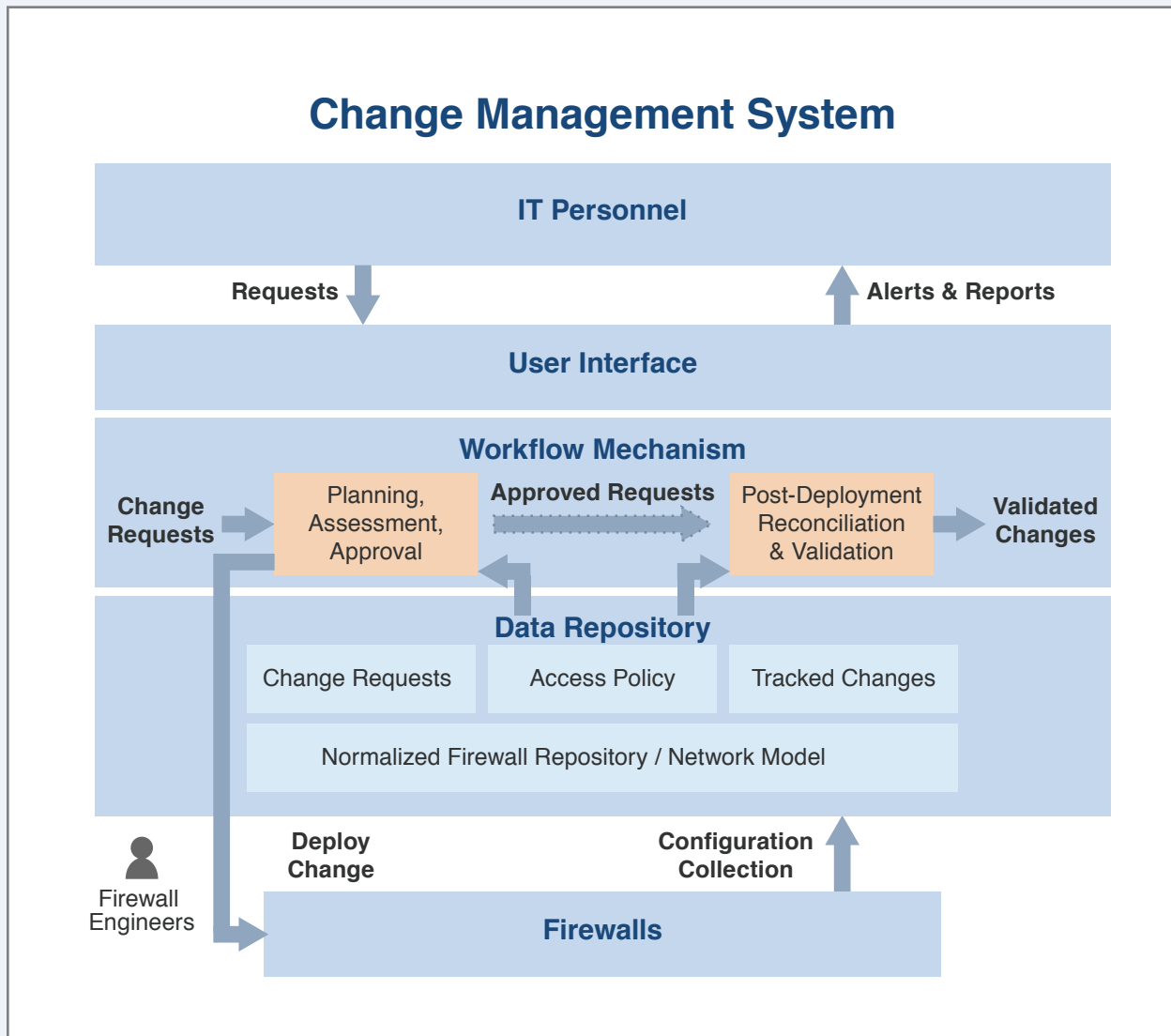


Figure 3 – Change Management System Components

The Change Management System consists of three major layers.

Layer 1: User Interface

The User Interface (typically a web interface) allows IT and business owners to feed change requests into the system. Following the process, technical and security team members can then view, augment, and approve the requests. Alerts can be established according to business policy and reports created for the various users of the system.

Layer 2: Workflow Mechanism

The workflow mechanism is responsible for transferring the request among the involved users according to the lifecycle phases of the request. In a firewall change management system two sets of built-in tools can assist the IT staff throughout the change process.

1. 1. Pre-Deployment tools assist with:
 - Planning and design — These tools help identify the firewalls to be changed and define the implementations details, such as rules or objects to be created or changed
 - Risk assessment — Automatic checks to assess security and compliance risks for the intended changes
2. Post-Deployment tools are responsible for:
 - Change tracking — Identify and record the actual changes performed to the firewall configurations
 - Change reconciliation and verification — Match the tracked changes with the change requests and identify deviations such as changes performed without an authorization, or change requests that have not delivered the intended result

Layer 3: Data Repository

In order to support the computation performed by the workflow tools, the system maintains:

- a repository of change requests
- a repository of up-to-date firewall configurations, represented in a normalized way
- a topological network model (optional)

The change request repository holds the details and the status of the requests, and their full history (audit trails). The repository enables searches for requests according to owner, requester, status, and request details.

A normalized firewall configuration repository is maintained automatically. Firewall configurations are collected on a regular basis (e.g., nightly) through communication with the firewall vendor's management platforms or with individual firewalls.

The repository can be extended to hold a topological model that puts firewalls in an accurate network context (see Figure 4). In this case the system automatically collects the configurations of additional network devices such as routers and load balancers and builds the topology, creating a normalized representation. With this network model, the workflow system can better understand the behavior of the firewalls and enables automated analysis of possible access from one area of the network to another, considering topology, routing rules, access lists, and NAT rules of firewalls along the route (a.k.a. "Access Analysis").

Why is Access Analysis so important?

Firewall change requests are about network access. To see if a request is already fulfilled (i.e. nothing to be done), find a network device that blocks the requested access, or to verify that the access request was fully achieved, network access has to be analyzed in an accurate way.

Another crucial capability of the change management system is its ability to check compliance of an access request with the corporate access policy.

The corporate access policy defines the acceptable network traffic. It is specified using a set of rules which typically relate to network zones. Firewall change management should provide a few out-of-the box policies that the organization can start with, and then customize if needed (e.g., NIST 800-41, PCI-DSS policy).

Following are examples of typical corporate policy rules:

- There should be no direct access from the Internet to internal zones (unless defined as exception)
- There should be no access from external zones to non-secure login services in the internal zones (Critical)
- The access from Internet to DMZ should be limited only to HTTP, HTTPS, SMTP, and DNS
- The number of destination addresses that have DNS access should not exceed 10

The corporate policy rules are represented in a formal way that can be used in automatic compliance checks of the change requests.

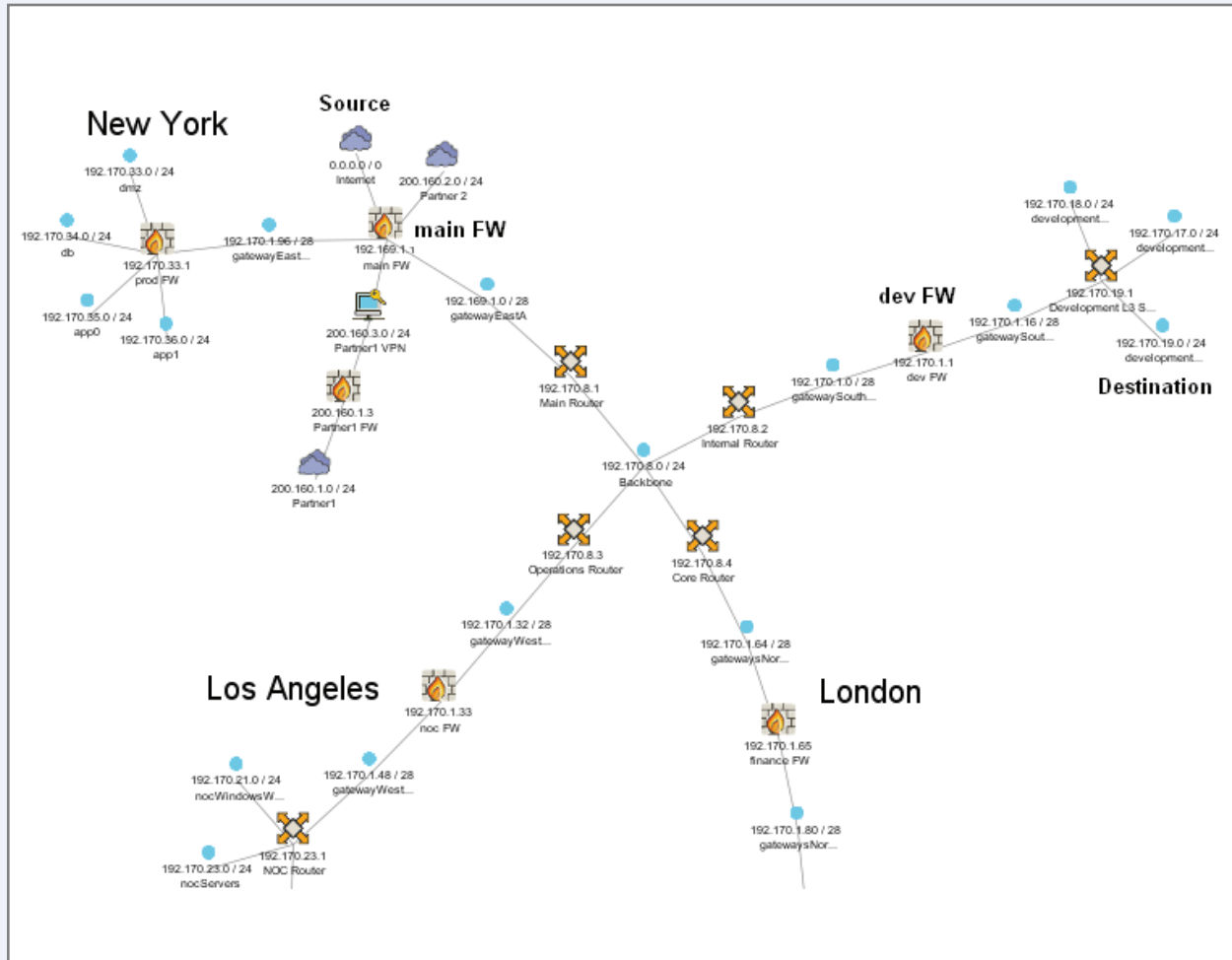


Figure 4 – Presenting a Topological Model on a Network Map

Working with the System

Step 1: Submitting a Change Request

Let us walk through a sample firewall change request (see Figure 5). In this example, an IT manager places a request to allow remote management of an external business service. A user authorized to make service changes submits a request that includes his details, a description of the request, its intended purpose, and a due date.

Step 2: Planning (Defining the Technical Details)

The network group receives the request and uses the workflow tools to identify firewalls that are relevant for a particular change. The system examines the routing scopes of firewall interfaces and optionally analyzes the topological model. Figure 6 shows that two firewalls were found to be relevant: dev FW and main FW.

The system also identified which of the relevant firewalls already allowed the required access. This is done using the Access Analysis capability of the system. Here, the requested access is possible through the dev FW but is blocked by the main FW. That means that only the main FW firewall has to be changed.

The screenshot shows the 'Skybox Change Manager' interface. At the top, there are navigation buttons: 'Save', 'Clone', 'Demote', 'Promote', 'Comments', 'Analyze', and 'Refresh'. A search bar for 'ticket #' is also present. Below the navigation is a tabbed interface with 'Request' selected. The 'Request' tab contains several sections: 'Requestor Information' (Name: John Brown, email: brown@skyboxseo, Department: Admin), 'Ticket Details' (Ticket Number: 334, Creation Time: 30/11/2010 11:13), 'Request Description' (Subject: Access is required to manage remotely App Server 3, Description: I need a remote telnet access from 194.90.1.5 to App Server 3. The access is needed for remote management of the server.), and 'Access Request Info' (Add/Remove buttons, Source Address: 194.90.1.5, Destination Address: 192.170.19.5, Destination Ports: 23/TCP).

Figure 5 – Feeding a Firewall Change Request

The screenshot shows the 'Requested Access' section of the Skybox Change Manager interface. It features a table with columns: 'Firewall Name', 'Source IP', 'Destination IP', 'Destination Ports', and 'Currently Access...'. The table is filtered for the request '194.90.1.5->192.170.19.5 (2 Items)'. Two rows are shown: 'dev FW' with a green checkmark and 'main FW' with a red X.

Firewall Name	Source IP	Destination IP	Destination Ports	Currently Access...
Request: 194.90.1.5->192.170.19.5 (2 Items)				
dev FW	194.90.1.5	192.170.19.5	23/TCP	✓
main FW	194.90.1.5	192.170.19.5	23/TCP	✗

Figure 6 – The system presents which firewalls are relevant for the request

In cases where access is already allowed through all relevant firewalls, the request can be returned to the requester with an indication that the requested access is already supported, thereby eliminating time spent on obtaining approval and defining implementation details. For each firewall that has to be changed, a dedicated request entry is generated by the system.

Step 3: Risk Assessment

The IT Risk group receives the planned request and assesses the risk and compliance of the request. To assist in this process the system automatically checks the compliance of each of the individual firewall requests against the corporate access policy and presents the results.

In Figure 7, the system determined that the requested access change of main FW is incompliant with the corporate access policy. It identifies that the source resides on an external network while the destination is within the internal networks, and hence the request violates two policy rules:

1. General Requirement: No direct access from external networks to internal networks (no exceptions were defined for this rule in the corporate access policy)
2. Critical Requirement: Blocking non-secure login services when accessing internal zones from external zones

The examiner of the request decides the risk level based on this information (in this case, High).

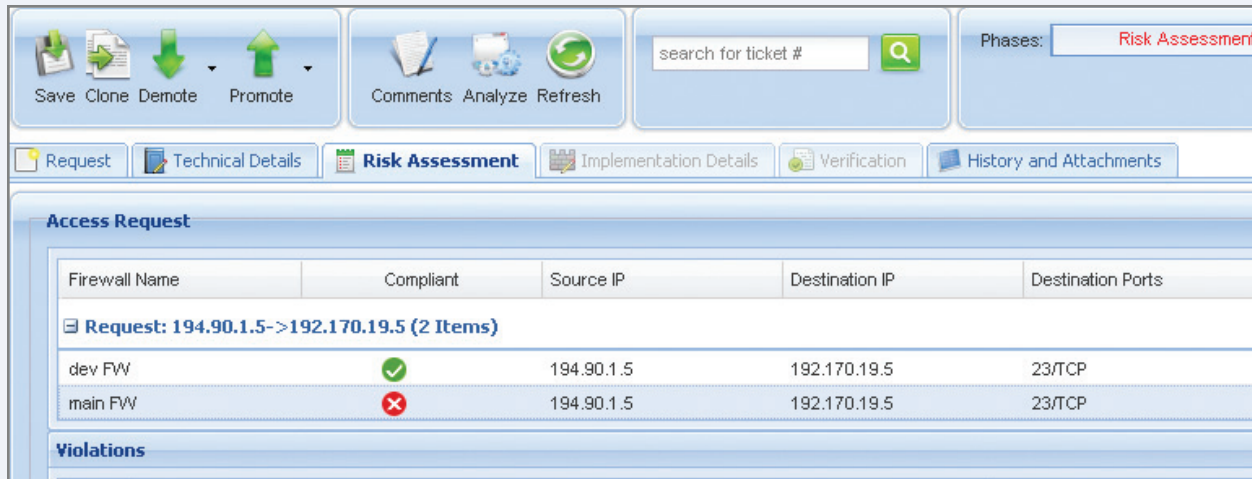


Figure 7 – The system identifies a critical violation of the corporate access policy

Step 4: Request Approval

Based on the assessed risk and the justification of the business need, the request is approved or transferred back to the planner for modifications (or in some cases, completely rejected). In this example, the examiner does not approve the telnet access as it violates corporate policy and recommends using the SSH protocol instead.

Step 5: Implementation Details

Once the request is approved, it is transferred to a firewall engineer who adds implementation details. The engineer should decide on questions such as:

- Should we implement the change using a new ACL rule or extend an existing rule?
- Where should we place a new ACL rule?
- Should we define a new object or extend the definition of an existing object?
- Do we need to add NAT rules? Which ones?

The system assists the operator in these decisions by searching through the current configuration of the firewall and identifies the relevant ACL rules and objects. After deciding on the implementation details, it can be checked for consistency with the original request and for compliance with rule and object guidelines.

Step 6: Deployment

A firewall engineer deploys the approved changes in the next service window. Using the system, the engineer can examine the list of change requests awaiting deployment and their respective details.

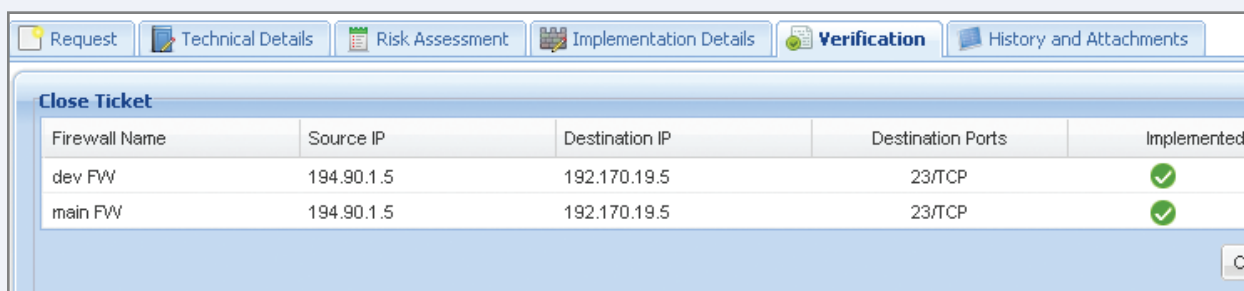
Step 7: Reconciliation and Verification

During the post-deployment phase, verification that change requests were implemented properly and enable the required access is performed.

The system automates what was before a time-consuming manual process. This is done as following:

- Changes to the firewalls are regularly tracked
- The identified changes are matched with the approved change requests
- It is verified that access required by the change requests is now possible (access check analysis)
- Unauthorized changes are identified

Building on our earlier example, Figure 8 presents the verification of on the change request after deployment. The request was modified to SSH access rather than telnet.



Firewall Name	Source IP	Destination IP	Destination Ports	Implemented
dev FW	194.90.1.5	192.170.19.5	23/TCP	✓
main FW	194.90.1.5	192.170.19.5	23/TCP	✓

Figure 8 – Automatic verification of the request after deployment

Access change requests that were verified by the system can be automatically closed or can await final user approval. The requester is informed via email and through the workflow system of the completion of the change request. Unauthorized changes and change requests that were not implemented properly are reported to the appropriate users.

Skybox's Unique Approach

Skybox Security offers a flexible solution to solve the enterprise challenges of firewall change management. The solution combines Skybox Change Manager, a web-based firewall change workflow system, with Skybox Firewall Assurance, a comprehensive firewall analysis and auditing tool.

Skybox Change Manager integrates firewall planning and risk assessment tools into the change request lifecycle, helping IT organizations define, evaluate, and manage every stage of the change process. The Skybox solution automatically collects and normalizes firewall configuration data, builds a topological model if desired, evaluates corporate access policy, and performs access analysis and policy checks.

Organizations looking to deploy a complete firewall change management solution can choose between two main deployment approaches:

1. Deploy Skybox Change Manager as a complete solution for firewall change requests in the organization
2. Continue to use an existing ticketing system for change management across the organization (e.g., a BMC Remedy-based solution), and integrate it with Skybox solution to perform the firewall planning, risk assessment and verification steps. The Skybox platform has the built-in capabilities for a seamless integration with an external ticketing system pulling information from the external system and returning status and details.

In addition, Skybox Change Manager communicates with the Skybox platform via a published web-services API. Skybox analytical services (access analysis, access compliance, searches through ACL rules and objects, etc.) can be called from any product developed by the customer or a third party.

When deciding on the best deployment approach, a consultation with Skybox's Professional Services team is recommended. Skybox Professional Services has extensive experience in enterprise deployments and integration with third-party tools and home-grown services.

References

Reference # 1 — “Approximately 80% of the IT budget is spent on operations, and a frightening proportion of this 80% is wasted by inefficiency.”

Forrester Research, “Knocking The NOC: Enter The New Operations Center”, April 30, 2009

Whitepaper: “How to Painlessly Audit Your Firewalls,” Skybox Security, Inc.

<http://www.skyboxsecurity.com/resources/white-papers/how-painlessly-audit-your-firewalls>

Product Demonstration: “Skybox Firewall Assurance Overview,” Skybox Security, Inc.

<http://www.skyboxsecurity.com/resources/product-demos/skybox-firewall-assurance-overview-930-minutes>

Firewall Assurance Datasheet, Skybox Security, Inc.

<http://www.skyboxsecurity.com/resources/data-sheets/skybox-firewall-assurance>

Change Manager Datasheet, Skybox Security, Inc.

<http://www.skyboxsecurity.com/resources/data-sheets/skybox-change-manager>

“The Standard of Good Practice,” Information Security Forum

<https://www.isfsecuritystandard.com/SOGP07/index.htm>

COBIT 4.1

<http://www.isaca.org/Knowledge-Center/cobit/Pages/Downloads.aspx>

Control Objectives; AI2.9 Applications Requirements Management; AI3.3 Infrastructure Maintenance; AI7.9 Post-implementation Review; DS9.2 Identification of Maintenance of Configuration Items

ISO 27001

<http://www.iso27001security.com/html/27002.html>

Chapter 9: Developing and Maintaining In-House Software; Managing Change Control Procedures
Requirement A.10.1.2 Change Management

ITIL

<http://www.itil-officialsite.com/home/home.asp>

ITIL v3 Change Control and Management Best Practices

NIST

<http://csrc.nist.gov/publications/PubsSPs.html>

NIST SP 800-53 Controls: CM-1, CM-3, CM-4, CM-5, CM-9

FISMA

<http://csrc.nist.gov/groups/SMA/fisma/index.html>

PCI DSS Requirement

<https://www.pcisecuritystandards.org/>

Requirements 1, 6, 11