skybox security

How to Painlessly Audit Your Firewalls

An introduction to automated firewall compliance audits, change assurance and ruleset optimization

May 2010

Executive Summary

Firewalls have become victims of their own success. These ubiquitous network security devices are the first line of defense for the business network, examining an endless stream of network traffic against a set of established rules. Over time, the exponential growth in web applications, e-commerce, communication tools, and networked business applications has led to a similar exponential growth in firewall complexity. In a typical organization today, a single firewall may be configured with thousands of rules to define network access policies, allowed services, routing rules, and more.

Maintaining good firewall configurations is a difficult challenge for even the most experienced network administrator. Even one firewall misconfiguration can result in a grave security, network availability, or regulatory compliance issue. With thousands of firewall rules and potentially tens or hundreds of firewalls in a large organization, it is difficult for any IT team to examine firewalls effectively and manage firewalls to ensure that the organization network is protected and in compliance.

Regular firewall auditing has become an essential part of firewall management. Establishing and effective firewall audit program requires defining policies, collecting firewall data, and evaluating the firewall data for policy violations and other issues. Due to scale alone, conducting regular manual firewall audits in an enterprise can be time- or cost-prohibitive, requiring weeks of IT resource time each year, per firewall.

In addition to time and cost concerns, firewall audit processes must take into account other challenges. Frequent configuration changes must be checked to ensure that they do not introduce potential risk exposures. Changing compliance and audit requirements from regulations and best practice frameworks such as PCI DSS, FISMA, NIST, SOX, COBIT, NERC and others make it difficult for firewall administrators to keep up with the latest guidelines. Against these kinds of challenges, it is no longer feasible for most organizations to conduct firewall audits manually. Automated firewall auditing solutions are essential, allowing IT administrators to quickly conduct compliance audits as often as necessary to ensure compliance, evaluate requested firewall changes before they are implemented, and identify ways of optimizing a firewall deployment to ensure availability and best performance.

Utilizing patented modeling and simulation technology, Skybox provides fast and effective solutions for automated firewall assurance for organizations with a few to hundreds of firewalls.

This whitepaper will examine the benefits of firewall auditing, provide guidelines for conducting effective firewall audit, discuss the challenges inherent in a manual firewall audit process, and present the benefits of automated firewall auditing solutions.

Table of Contents

Why Are Firewall Audits Needed?

Firewalls have been the first line of network defense for nearly 20 years. Early firewalls were simple packet filters, using a small set of rules to determine whether certain traffic would be allowed in to the network. Over time, the exponential growth in the number and type of network-enabled applications, web-based services, communication tools and more has led to an overwhelming number and array of possible firewall rules and settings. Today's firewalls now fill the role of 'traffic cop' in intersections with hundreds of crossroads and thousands of traffic rules.

A single erroneous rule in a firewall configuration could lead to devastating impact on the risk level of the organization. Security, regulatory compliance, and network availability and performance may all be impacted by firewall settings and dependencies between rules. According to a recent report by Forrester Research, as many as 80% of firewalls examined in a data breach investigation were misconfigured.

A few examples will illustrate the potential effects:

Scenario	Business Impact
A firewall access rule change leads to the unintentional blocking of an online banking service	Prevents consumers from accessing their accounts
A new business-to-business service is introduced, requiring new permissive firewall rules	Exposes the organization to serious attacks on intellectual property assets
A network connection is now allowed from the Internet to the internal ERP system to satisfy new supply chain management needs	Introduces severe violations of the corporate *Network Security Policy.* The organization will fail the next audit since the firewall configuration now deviates from policy requirements
A firewall accumulates hundreds of changes over the years, without a periodic clean-up	Slows network performance dramatically due to a complex set of firewall rules that are no longer needed

In order to prevent the negative impacts of these common scenarios, firewall administrators must frequently audit firewalls and change firewall rules and configuration settings to ensure security, compliance, availability, and optimal performance.

Firewall Audit is the process of analyzing a firewall configuration for the purpose of answering the following type of questions:

1. Is my network security policy properly enforced by each firewall? If not, how can I quickly fix the most important violations?
2. Is the firewall that protects cardholder data configured according to the PCI DSS requirements?
3. Which firewall rules are not used and therefore can be eliminated? Which rules can be re-ordered or consolidated in order to improve performance?
4. Will a proposed network change introduce any new security exposures or availability problems? What is the best way to implement the proposed change?

A firewall audit process is not only important to ensure the security, availability, and performance of the organization network, but it is also mandated by many regulatory compliance requirements and best practices.

The mandatory requirements for configuration assurance fall into two main categories:

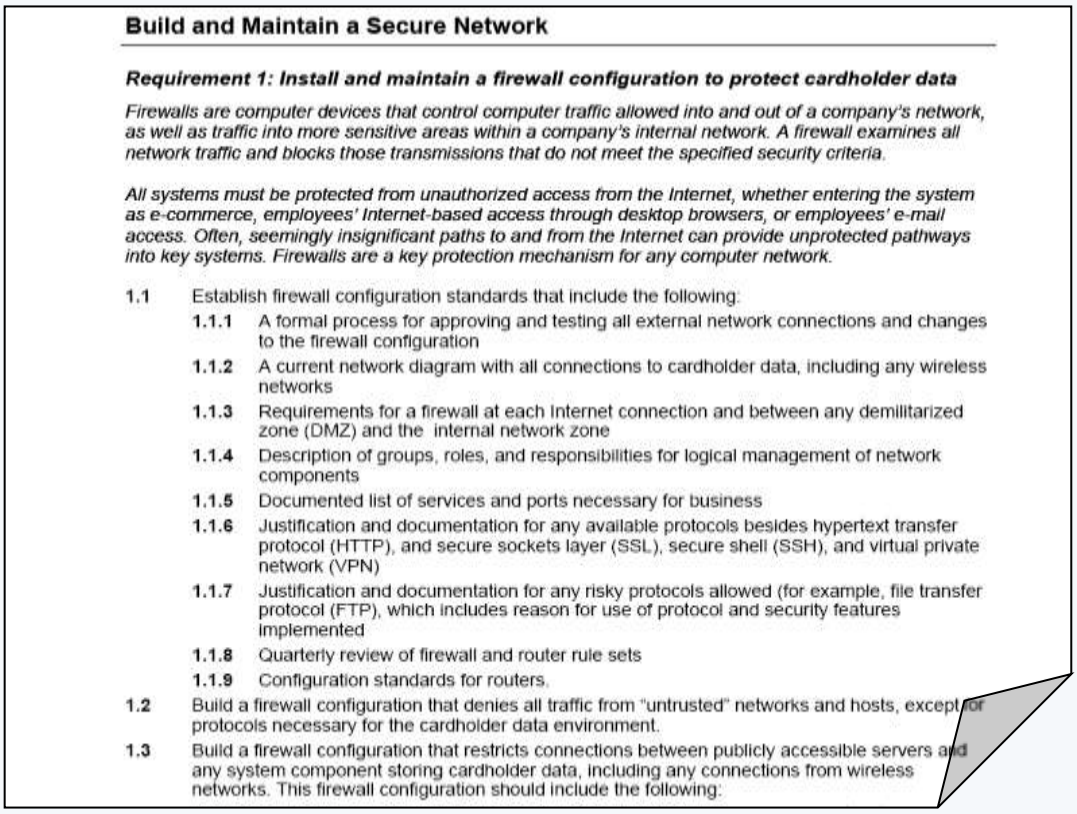
1. Configuration compliance with network security policies
   a. Specific requirements such as in the case of PCI DSS, SANS, and NIST SP 800-41
   b. Corporate-defined policies as required by SOX/COBIT, ISO 27001, NERC, and others
2. Implementation of change impact analysis controls – can be found in COBIT, ITIL , ISO 27001, NIST, and others

PCI DSS Compliance Requirements

The PCI Data Security Standard provides specific instructions as to the proper installation and maintenance of firewalls that protect cardholders' data. Requirement 1 refers to the need for:

- A formal process for approving and testing all external network connections and changes to the firewall configuration
- Documenting a list of services and ports necessary for business (the "access policy")
- Justification or documentation for any risky protocol
- Ensuring proper network zoning in order to protect systems with card holder data
- Periodic reviews of configurations (at least every 6 months)

Each of these activities can be addressed as part of a defined firewall audit process.



Build and Maintain a Secure Network

Requirement 1: Install and maintain a firewall configuration to protect cardholder data

Firewalls are computer devices that control computer traffic allowed into and out of a company's network, as well as traffic into more sensitive areas within a company's internal network. A firewall examines all network traffic and blocks those transmissions that do not meet the specified security criteria.

All systems must be protected from unauthorized access from the Internet, whether entering the system as e-commerce, employees' Internet-based access through desktop browsers, or employees' e-mail access. Often, seemingly insignificant paths to and from the Internet can provide unprotected pathways into key systems. Firewalls are a key protection mechanism for any computer network.

1.1 Establish firewall configuration standards that include the following:

- **1.1.1** A formal process for approving and testing all external network connections and changes to the firewall configuration
- **1.1.2** A current network diagram with all connections to cardholder data, including any wireless networks
- **1.1.3** Requirements for a firewall at each Internet connection and between any demilitarized zone (DMZ) and the internal network zone
- **1.1.4** Description of groups, roles, and responsibilities for logical management of network components
- **1.1.5** Documented list of services and ports necessary for business
- **1.1.6** Justification and documentation for any available protocols besides hypertext transfer protocol (HTTP), and secure sockets layer (SSL), secure shell (SSH), and virtual private network (VPN)
- **1.1.7** Justification and documentation for any risky protocols allowed (for example, file transfer protocol (FTP), which includes reason for use of protocol and security features implemented
- **1.1.8** Quarterly review of firewall and router rule sets
- **1.1.9** Configuration standards for routers.

1.2 Build a firewall configuration that denies all traffic from "untrusted" networks and hosts, except for protocols necessary for the cardholder data environment.

1.3 Build a firewall configuration that restricts connections between publicly accessible servers and any system component storing cardholder data, including any connections from wireless networks. This firewall configuration should include the following:

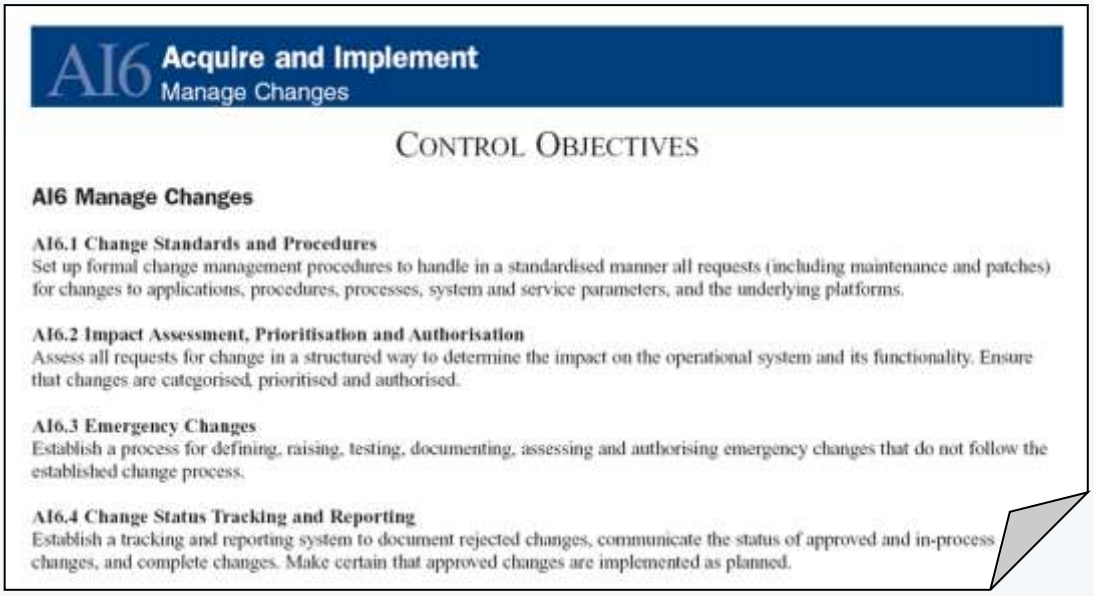
Figure 1 PCI DSS Requirement #1

COBIT Framework

The next example is taken from The Control Objectives for Information and related Technology (COBIT), which is a set of best practices (framework) for information technology (IT) management.

COBIT, which is adopted as the default framework for Sarbanes Oxley Act implementation (SOX), includes specific *control objectives* around change management, proactive security testing, and monitoring internal controls. These control objectives are relevant for the entire IT infrastructure, including firewalls.

Firewall configuration analysis should be done before any change is deployed in order to assess the potential exposures that may be introduced by the requested configuration changes. This process can satisfy the COBIT requirements for change impact analysis.



AI6 Acquire 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 2 COBIT - Change Management Control Objectives

How to Audit a Firewall? ("Firewall Audit 101")

As explained in the previous section, frequent and thorough firewall audits are critical to reduce business risk exposures on an on-going basis, and are also required for to demonstrate compliance with many information security regulations and best practices.

A typical firewall audit program incorporates the following steps:

1. Define network access policy
2. Retrieve firewall configuration information
3. Map network interfaces to policy zones
4. Analyze the firewall against the organization's access policy – detect violations, highlight compliance level
5. Find unused and redundant rules – configuration optimization

Acme Power - Example

To illustrate the firewall audit process, we will use an example of a fictitious organization called *Acme Power.* Acme power is a public company that distributes electric power to consumers around the country. Acme is subject to many regulations and industry standards, including SOX (as a public company), NERC CIP (as a power company), PCI DSS (as utility bill payments may be made via credit card charges), and more.

To simplify the example, we will focus on one firewall out of the many utilized by Acme Power. This Internet Firewall regulates network traffic between the Internet, a DMZ network, and a server farm that provides applications for billing and customer service.

1. Define network access policy

Before beginning a firewall audit, there must be a defined corporate policy in place to establish the do's and don'ts of network access. This policy is typically a superset of the security requirements which are specific to the business, plus regulatory requirements (e.g. PCI DSS) and industry best practice guidelines (e.g. NIST).

A network access policy has multiple components:

- Network zones – segmentation of the organization network (and its eco-system) into logical zones such as Internet, DMZ, Server Farms, Corporate Services, Partners, etc.
- Access policy rules – set of rules that define the types of traffic which are allowed or denied from one zone to another

Acme Power has more than twenty different logical zones in its policy, of which three are relevant for the Internet Firewall: **Internet**, **DMZ** (IP range: 12.0.12.0/24), and **Server Farm** (IP range: 192.168.10.0/24)

Out of hundreds of Acme policy rules, over fifty are relevant for these zones. The following table lists a few of them:

Network Security Policy:

#	Source zone	Destination zone	Services/Ports Allowed	Comment
1	Internet	Server Farm	None	No direct connection allowed from the Internet to the Server Farm – satisfies PCI DSS 1 requirements
2	Internet	DMZ	SMTP – limited to 5 IP addresses HTTP and HTTPS – limited to default ports	
3	220.220.110.0/24	DMZ	HTTPS – limited to 1 IP address and port 8443	Web server available for a strategic partner of Acme Power
4	DMZ	Server Farm	MySQL database – default port (3306)	
5	Server Farm	Internet	None	No outbound communication is allowed from the Server Farm to the Internet
6	Internet	DMZ	DNS/UDP allowed	TCP is not allowed due to "zone transfer" vulnerabilities

2. Retrieve configurations

Once a network access policy is established, configuration files must be retrieved from the firewalls or their management software to build the following set of information:

- Network interfaces
- Firewall access rules, aka Access Control List (ACL)
- Routing rules (optional, but useful if routing is not obvious)
- Additional rules for NAT VPN etc. (if any)

The configuration for Acme Power's **Internet Firewall** has the following network interfaces and firewall rules (ACL):

Network interfaces:

#	Interface name	Address / Mask	Type	Default Gateway
1	ISP	12.0.1.10/30	WAN	12.1.0.255
2	DMZ1	12.0.12.1/24	LAN	12.1.0.255
3	Internal	192.168.10.1/24	LAN	12.1.0.255

Firewall rules:

#	Source	Destination	Services	Action	Direction	Comment
1	12.0.12.0/24	192.168.10.0/24	Not 3300-3310/TCP	Deny	Inbound	DMZ
2	12.0.12.0/24	192.168.10.10-192,168.10.15	Any	Allow	Inbound	
3	Any	12.0.12.0/16	25, 80, 443/TCP	Allow	Inbound	
4	192.168.0.0/16	Any	80, 443/TCP	Allow	Outbound	Outbound communication is allowed from internal users on port 80 and 443
5	220.220.110.0/24	12.0.12.0/24	1000-10,000/TCP, UDP	Allow	Inbound	Allow inbound communication from strategic partner network to the DMZ
6	12.0.12.0/24	192.168.10.12	3306/TCP	Allow	Inbound	
..						
99	Any	12.0.12.0./24	53/TCP, UDP	Allow	Inbound	
100	Any	Any	Any	Deny	Both	

Note: Actual firewall configurations tend to be significantly more complex than this illustration.

3. Map network interfaces to policy zones

In order to find policy violations we need to understand which policy rules have to be analyzed against the firewall configuration. This is done by mapping each network interface to a policy zone and then selecting the policy rules which fits any combination of two interfaces.

The following is the straightforward mapping of Acme Power policy zones to each one of the interfaces.

Network interfaces mapping to Policy Zones:

#	Interface name	Address / Mask	Policy Zone
1	ISP	12.0.1.10	*Internet*
2	DMZ1	12.0.12.1	*DMZ*
3	Internal	192.168.10.1	*Server Farm*

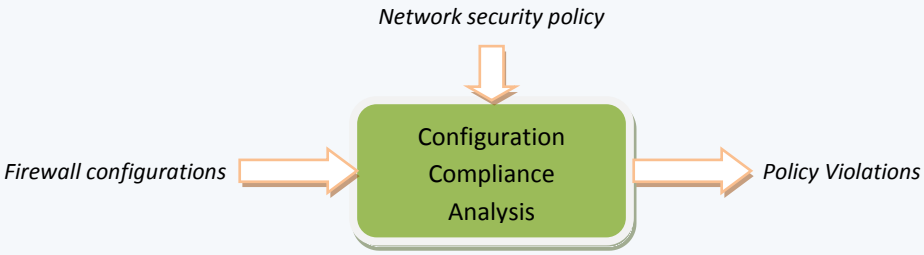
Now we have the information to know which policy rules apply to which pair of network interfaces of *Internet Firewall*.

Network security policy:

#	Source zone	Destination zone	Services/Ports Allowed	Source Interface	Destination Interface
1	Internet	Server Farm	None	*ISP*	*Internal*
2	Internet	DMZ	SMTP – limited to 5 IP addresses HTTP and HTTPS – limited to default ports	*ISP*	*DMZ1*
3	220.220.110.0/24	DMZ	HTTPS – limited to 1 IP address and port 8443	*ISP*	*DMZ1*
4	DMZ	Server Farm	MySQL database – default port (3306)	*DMZ1*	*Internal*
5	Server Farm	Internet	None	*Internal*	*ISP*
6	Internet	DMZ	DNS/UDP allowed	*ISP*	*DMZ1*

4. Compliance and security analysis

Now, that we have a security policy, a firewall configuration, and mapping of the network interfaces to the policy rules, it is possible to begin configuration compliance analysis.



Compliance analysis is done by reviewing every rule in the security policy against the actual rules within the firewall configuration (ACL) in order to find violations of three main types:

1. Firewall allows network traffic which is forbidden by the security policy of the organization
2. Firewall allows network traffic which is broader (in terms of IP addresses and/or ports) then allowed by the security policy
3. Firewall denies network traffic which is required for availability of network services

The compliance analysis may become very complex, as a single firewall may have hundreds or thousands of rules and ensuring the compliance to even one policy rule is an error-prone and resource consuming process.

Policy violations can be either fixed by network security operator, or can be accepted as “exceptions” to the policy for a certain period of time, until the right solution is found and can be implemented.

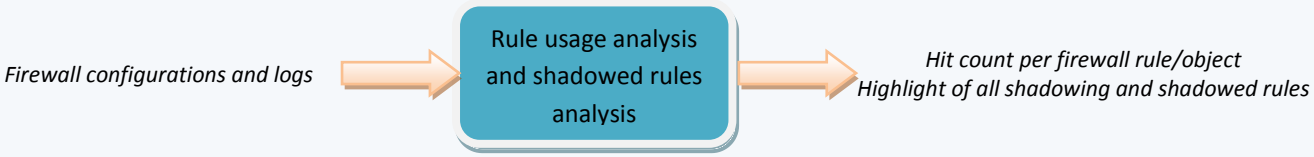
Returning to the Acme Power Internet Firewall example, here are few found violations to the policy:

Firewall rules:

#	Source	Destination	Services	Action	Direction	Acme's policy violations	Details
1	12.0.12.0/24	192.168.10.0/24	Not 3300-3310/TCP	**Deny**	Inbound	No violations	
2	12.0.12.0/24	192.168.10.10-192,168.10.15	Any	**Allow**	Inbound	Violates policy rule #4 which permits only MySQL traffic on port 3306.	The combined effect of firewall rules #1 and #2 is that servers with IP addresses of 192.168.10.10-192,168.10.15 can be accessed in any ports 3300-3310, which is broader than allowed by the policy
3	Any	12.0.12.0/16	25, 80, 443/TCP	**Allow**	Inbound	No violations	
4	192.168.0.0/16	Any	80, 443/TCP	**Allow**	Outbound	Violates policy rule #5 which doesn't permit any traffic from the Server Farm to the Internet	This firewall rule allows outbound connection from 192.168.0.0/16 which includes the Server Farm (192.168.1.0/24)
5	220.220.110.0/24	12.0.12.0/24	1000-10,000/TCP, UDP	**Allow**	Inbound	Violates policy rule #3 which permits traffic only to one server in the DMZ and only to port 8443	This firewall rule permits traffic to the entire DMZ and to wide port range.
6	12.0.12.0/24	192.168.10.12	3306/TCP	**Allow**	Inbound	No violations	
..							
99	Any	12.0.12.0./24	53/TCP, UDP	**Allow**	Inbound	Violates policy rule #6 which doesn't permit any DNS/ TCP traffic	This rules allows both UDP and TCP traffic on port 53 (DNS)
100	Any	Any	Any	**Deny**	Both		

5. Find unused and redundant rules – configuration optimization

A thorough review of firewall rules in conjunction with rule usage log information can reveal potential security holes and opportunities for configuration optimization. The results of this analysis are recommended opportunities to optimize the firewall configuration by removing, consolidating, or reordering unused or rarely used rules, redundant rules, and shadowed rules.



This analysis is composed of two main tasks:

1. Counting number of hits per firewall rule and object, within a certain window of time – aka rule usage analysis
2. Finding all firewall rules that are shadowed by other rules or made redundant by other rules

Similar to compliance analysis, these evaluation tasks can be very complex and time consuming. Counting the number of hits requires the analysis of millions lines of logs daily and correlating them with a complex firewall ruleset. Finding shadowed rules require analysis of the interrelationship between any pair of firewall rules – which could represent millions of combinations in the case of a complex firewall with thousands of rules.

By analyzing the Acme Power logs for a certain period of time and reviewing the ruleset, we reach the following conclusions:

#	Source	Destination	Services	Action	Direction	Rule Hit Count	Rule Shadowing Analysis	Conclusions
1	12.0.12.0/24	192.168.10.0/24	Not 3300-3310/TCP	Deny	Inbound	25		Need to find out which servers are trying to communicate to forbidden ports
2	12.0.12.0/24	192.168.10.10-192,168.10.15	Any	Allow	Inbound	89,339		
3	Any	12.0.12.0/16	25, 80, 443/TCP	Allow	Inbound	1,010,211		Due to high hit-count, this rule should be considered to be earlier in the ruleset
4	192.168.0.0/16	Any	80, 443/TCP	Allow	Outbound	245,932		
5	220.220.110.0/24	12.0.12.0/24	1000-10,000/TCP, UDP	Allow	Inbound	0		Due to zero hit-count, this rule should be considered to be removed, unless still required by the business
6	12.0.12.0/4	192.168.10.12	3306/TCP	Allow	Inbound	0	This rule is shadowed by rule #2	Rule can be eliminated (while fixing rule #2 due to its policy violations)
..								
99	Any	12.0.12.0./24	53/UDP	Allow	Inbound	3,990,208		Due to high hit-count, this rule should be considered to be earlier in the ruleset
100	Any	Any	Any	Deny	Both	25,000,000		

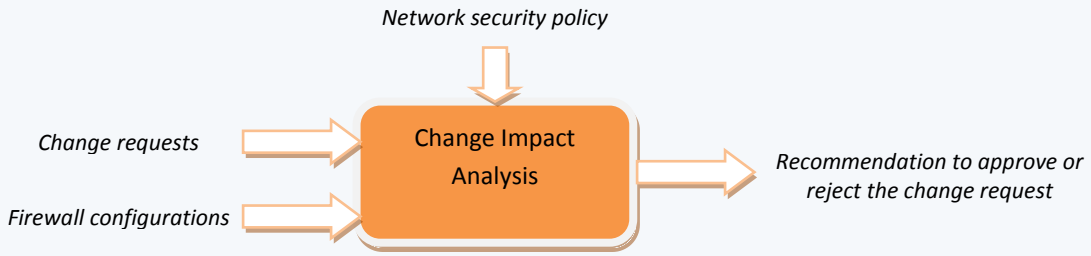
Safe Change Management with Firewall Audit Techniques

In order to accommodate network connectivity requirements, firewalls are changed very frequently, once or twice a month on average. These changes are driven by:

- Business needs –enable new business applications, or to decommission old ones
- IT Operations needs – support changes in network architecture and standards
- Security needs – tighten network traffic to the minimum required by the business and IT operations

These frequent change requests (especially in cases organizations have tens or hundreds of firewalls) require careful planning, impact analysis, approval, execution, and tracking.

Though this white paper doesn't focus on firewall change management, it is worthwhile to mention that firewall audit techniques can be utilized for "change impact analysis", which is a required control by security best practices and control frameworks such as ISO, NIST, COBIT, and ITIL to name a few.



Compliance analysis, as explained in an earlier section, can allow the network security operator to verify that the change request doesn't violate the network security policy, and whether the change is actually needed (i.e. perhaps connectivity is already allowed in the network, or allowed by the firewall, and the change is not needed), before the change has been made – aka "what –if analysis."

Manual versus Automated Firewall Audits

While firewall auditing is a required and very helpful process to prevent and mitigate risk exposures, conducting manual audits against all firewalls in an organization often raises significant operational challenges.

A single firewall audit may take days of work due to the complexity of the firewall configuration. Even a single change request may require hours of work to plan the change and to perform comprehensive impact analysis. The following table illustrates the typical time required to examine an average firewall with a few hundred rules.

Process	Typical Frequency (limited by available resources)	Amount of time per iteration (per firewall)	Time per year (per firewall)
Configuration compliance analysis	Once a quarter	2 days	8 days
Change impact analysis	Twice a month	2 hours	6 days (24 x 2 hours a year, assuming 8 working hours a day)
Configuration optimization	Once a year	4 days	4 days
Total			**18 days**

At an estimated resource requirement of 18 days per year to sufficiently audit one firewall, it may cost as much as $15,000 per year in internal resource costs, or as much as $30,000 per year if an external resource is required. What if the organization has tens or hundreds of firewalls? What if the organization needs to perform compliance analysis weekly or optimize the firewalls quarterly or even more often? It is easy to see how manual firewall audits may quickly become cost-prohibitive.

Several other factors may amplify the challenges of manual audits:

1. Complexity. The example above assumes "average" firewall configurations. There are many firewalls in use with configurations that consists of thousands of rules, rendering manual audits essentially impossible
2. Multi-vendor environments. Many organizations end up with several firewall vendor platforms in use, either the result of different firewall generations in the IT infrastructure, or through M&A activity. Each new vendor platform requires specific knowledge to understand and analyze the firewall settings
3. IT staff churn. Manually auditing groups of firewalls is a time-consuming, mundane activity. It is a challenge to retain skilled resources if firewall audits start to consume a significant portion of their time, limiting their involving in more interesting IT challenges.
4. Human error. Any manual analysis process is prone to mistakes, and the accuracy of a manual firewall audit depends significantly on the expertise and motivation of the administrator

Organizations are left with an unbearable trade-off between high risk exposures and possible non-compliance, and unaffordable resource requirements, as illustrated in the figure below.

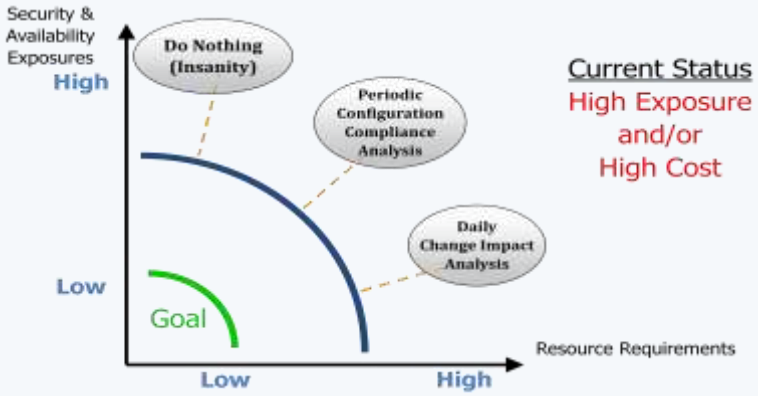


Figure 2 Manual Firewall Audit Trade-Off

The only way to achieve the goal of low firewall management cost and low risk exposure for the organization is by automating the steps needed to conduct firewall audits.

The benefits of automating firewall audits are numerous:

1. Less downtime due to effective and accurate change management process, with changes analyzed in advance
2. Fewer security risks due to automated and frequent compliance assessment of the network security policy
3. Lower compliance costs due to automated reporting, and avoidance of possible fines and reputation impacts
4. Longer lifespan of firewalls due to performance optimization

In moving to an automated firewall audit approach, Acme Power realizes significant improvements such as:

- Reducing the time for firewall analysis from 2-4 days to less than one hour
- Reducing the speed for a single change analysis from 2 hours to 5 minutes
- Improving analysis accuracy from 70% to 90%
- Reducing the window of risk exposures from weeks to minutes

Plus, using an automated solution allows compliance audits to be conducted as frequently as necessary to maintain continuous compliance.

Skybox's Unique Approach

Skybox Security has a proven firewall assurance solution to conduct accurate, automated, and highly scalable firewall audits. The Skybox approach offers many distinctive capabilities, including:

Capability	Benefits
Vendor and platform independent	Allows consistent analysis and reporting for all firewall products
Automation from A to Z	High ROI and significant resource saving
Powerful network access policy editing, and out of the box policies	Easy transition from manual process to automated solution
Flexible and non-intrusive data collection	Quick time to deploy
Lifecycle management of policy violations	Enables a controlled ramp-up for compliance initiatives
Accurate and industry fastest algorithms	Saves 80-90% of the time spent on audit, change assurance, and optimization; eliminate configuration errors
Scalable architecture	Provides a solution to any size organization
Integrated with enterprise change management process	Enables change assurance, without the need to build change management process from scratch
Network modeling – enables firewall analysis in the context of the entire network (optional)	Makes change planning and assessment more accurate; balances security & availability exposures; quick troubleshooting and root-cause analysis

For more information, see http://www.skyboxsecurity.com/firewallcompliance.

Summary

Over time, firewall audits have evolved into an essential process for any organization. Firewall audits can identify potential security issues, help ensure adherence to compliance requirements and industry best practices, identify potential errors of planned changes, and improve firewall performance and network availability.

To maintain an effective firewall audit program, IT organizations must define network access policies, retrieve configuration data, map network interfaces, analyze configurations for policy violations, and examine rule usage. In practice, conducting a manual audit program for even a single firewall can require weeks of resource time. With large firewall deployments, complex firewall rules, and limited resources and budget, the only way to keep firewalls in compliance and reduce possible security or availability exposures is by using an automated solution.

An automated firewall auditing solution can reduce the resources required for firewall configuration audits, change assurance, and ruleset optimization by more than 80%. In addition, the window of exposure (measured by the time between assessments) can be reduced by at least 90%.

[1] Kindervag, John; *Market Overview: Firewall Auditing Tools*; Forrester Research; July 30, 2009