



FIREWALL MANAGEMENT: 5 CHALLENGES EVERY COMPANY MUST ADDRESS

An AlgoSec Whitepaper



Table of Contents

Introduction	3
Business Challenge #1: Assessing the risk of the firewall policy	4
Business Challenge #2: Managing firewall changes	5
Business Challenge #3: Maintaining optimized firewall rulesets	7
Business Challenge #4: Keeping up with rules and regulations	8
Business Challenge #5: Proving where things stand	9
Moving Forward	10



Introduction

More than two decades into utilizing network firewalls, and we're still struggling to properly manage and use them to their fullest potential. In today's world of information-driven businesses there's a lot more that can go wrong— and a lot more to lose—when it comes to firewalls, firewall management and overall network security. Network environments have become so complex that a single misstep on a critical firewall can take the entire network offline and expose your business to cyber attacks.

Improperly managed firewalls create some of the greatest business risks in any organization. Often, the risks are things you don't find out about until it's too late, such as:

- Outdated firewall rules that allow unauthorized network access and cyber attacks
- Gaps in compliance with industry and government regulations
- Improper firewall rule changes that break business applications

One unique thing about firewall-related risks is that they don't require sophisticated hacking skills to be exposed. In fact, your own team can be your organization's worst enemy. Simple errors and oversights in the process of managing your firewalls can cause problems like opening up the network perimeter to security exploits, and creating business continuity issues. Add network complexity into the mix, combined with all the other duties you and your team are responsible for, it becomes clear that firewall management is a business challenge that you need to address properly once and for all.

Business Challenge #1: Assessing the risk of the firewall policy

As networks are becoming more complex and firewall rulesets continue to grow in size, it is increasingly difficult to identify and quantify the risk that is introduced by misconfigured or overly permissive firewall rules.

The major contributor to firewall policy risks is lack of the proper understanding of exactly what the firewall is doing at any given time. Even if traffic is flowing and applications are working, it doesn't mean you don't have unnecessary exposures.

Serious IT and network security professionals are continually thinking about the choices they're making today, and the resulting risks those choices can create moving forward. Everything you and your team do related to your firewall policies moves your network either towards better security or increased risks. Even the most experienced firewall administrators can make honest mistakes. You'll never really know where things stand until you have the proper visibility.

The Solution:

The best approach for minimizing firewall policy risks is to ensure you—and management—understand what there is to lose. Use smart network and firewall architectures to your advantage and then lean on automated management tools to help find and fix the security risks before they grow out of control. Solid automated management tools can employ widely-accepted firewall best practices and analyze your current environment to highlight gaps and weaknesses. Some tools can also help tighten overly permissive rules (e.g., "ANY" service) by pinpointing the traffic that is actually flowing through any given rule.

Combining manual policy analysis with the right tools allows you to be proactive with firewall security rather than finding out about the risks once it's too late.

Business Challenge #2: Managing firewall changes

In IT, things are constantly in a state of flux. Managing all the changes is one of the biggest problems that businesses face. As with most things in IT, there's not a simple solution for managing changes by default—especially when it comes to firewalls. Still, not properly managing changes can lead to serious business risks, from issues as benign as legitimate traffic being blocked, all the way to the entire business network going offline and businesses being hacked.

Many factors contribute to problems with firewall change management, but the main culprits are:

- 1. Lack of formal policies.** In the context of firewalls, rulesets—or policies—are often confused with formal information security policies. It's critical to know the difference and ensure you have an official policy for change management that includes all your firewalls within its scope.
- 2. Loose processes that aren't taken seriously.** It's one thing to have a policy stating “this is what we must do,” but quite another to have a formal set of steps for carrying out and enforcing that policy. Firewall change management requires detailed and concise steps that everyone must follow when changes are needed. Any exceptions need to be approved and documented.
- 3. Poor communication among IT staff.** Another serious barrier to network security success is poor communication among those responsible for keeping the firewall environment in check. It's also a large contributor to out-of-band changes that lead to firewall mishaps.
- 4. Not understanding the associated business risks.** It's imperative to know what the business is up against from the perspective of threats and vulnerabilities. What's often overlooked, however, is the impact poorly-managed firewall changes have on the business. A lot of money and effort is put into keeping the bad guys out, while we forget that we're often our own worst enemy.
- 5. Network complexity.** The sheer complexity of any given network can lead to a lot of mistakes, especially when it comes to multiple firewalls with complex rulesets. Complexity is the enemy of security, and you need to do whatever it takes to simplify your firewall environment and management processes.
- 6. Not understanding the impact of firewall changes.** Not analyzing and thinking through how even the smallest firewall changes are going to impact the network environment can have dramatic effects. Without thoughtful analysis you might not know things such as:
 - Which applications and connections your changes may break.
 - Which new security vulnerabilities are going to be introduced.
 - How performance and visibility are going to be affected.

A Case Study in Firewall Mismanagement

A recent incident at an e-commerce company, in which firewall changes went awry, provides good insight into how a few bad choices can lead up to a monumental failure.

The company was a core provider of ecommerce services to businesses in the U.S. One day, all e-commerce transactions in and out of their network ceased. The entire business was taken offline for a number of hours. It ended up being a few members of the firewall team who had made some out-of-band (and untested) changes to a core firewall that broke the communication between the ecommerce application and the rest of the Internet.

Because of the incident, executive management got involved and the responsible IT staff members were reprimanded. Hundreds of thousands of dollars later, the root cause of the outage was revealed: IT staff chose not to test their firewall changes—bypassing their “burdensome” ITIL-based change management procedures—and ignored the consequences.

The Solution:

If you can manage firewall changes consistently over time, then you’ve already won half the battle. You’ll not only have a more secure network environment, but you will allow IT to serve its purpose by actually facilitating business rather than getting in the way.

To manage firewall changes properly, you need to use a good set of tools in the right ways. To set up your team for success, it’s critical to have well-documented and reasonable policies and procedures, combined with technical controls that help with enforcement and oversight. The right automated tools can:

- Create and enforce workflows for the different processes of security policy changes.
- Leverage topology awareness to identify the firewalls that are affected by a proposed change.
- Simulate the change to proactively detect risk or compliance implications before the change is implemented.
- Reconcile change requests with the actual changes performed, to identify any changes that were performed “out of process.”

It is possible, to an extent, to think about—and analyze—the impact firewall changes will have on the business. The ideal way is to utilize built-in or third-party firewall management tools that allow you to test different scenarios before pushing them out to production.

Once such tools and processes are integrated with your overall change management function, you can set your business up for success instead of creating a “wait and see” situation, and “hoping” everything works out.

Simply put, if you don’t have the proper insight and predictability, then you’ll set up your business and yourself for failure.

Business Challenge #3: Maintaining optimized firewall rulesets

Maintaining a clean set of firewall rules is one of the most important firewall management functions, yet many businesses continue to struggle with it. Unwieldy rulesets are not just a technical nuisance—they also create business risks, including open ports and unneeded VPN tunnels, conflicting rules that create backdoor entry points, and an enormous amount of unnecessary complexity. In addition, bloated rulesets significantly complicate the auditing process, which often involves a review of each rule and its related business justification. This creates unnecessary costs for the business and wastes precious IT time.

Examples of firewall rules that can create problems include:

- Unused rules
- Shadowed rules
- Expired rules
- Unattached objects
- Rules that are not ordered optimally (e.g., the most hit rule is at the bottom of the policy, creating unnecessary firewall overhead)

These problems drive organizations to take on ad hoc firewall “cleanup” or “recertification” projects. The problems are also magnified in enterprises with numerous firewalls from various vendors. Such complexities contribute to a lack of visibility, poor accountability, and undetected network breaches.

Another interesting problem occurs when network administrators and security managers are asked for a copy of their network diagram. Quite often there is either no diagram, or the diagram is very outdated. Firewall rulesets are no different.

This isn’t necessarily the fault of one particular person, but more a side effect of IT staff working in a reactive mode, putting out fires rather than proactively managing their networks on a daily basis. This issue, combined with network complexity and IT politics, leads to mismanaged firewall rulesets and their associated business risks.

The Solution:

Just as firewall change management is a formal process where people are held accountable, firewall ruleset maintenance needs to become formalized as well. Proactive and periodic checks can help eliminate rulebase oversights, and allow you to maintain a firewall environment that facilitates security rather than exposes weaknesses.

To effectively manage your firewall rulesets, you need the right tools. The proper firewall management tools will provide you with the visibility needed to see which rules can be eliminated or optimized, and also see the implications of removing or changing a rule. They can also automate the process, eliminating the need for time-consuming and inaccurate manual checks.

You also need to ensure that you’re managing the rulesets on all of your firewalls. Picking and choosing certain firewalls is like limiting the scope of a security assessment to only part of your network. Your results will be limited, creating a serious false sense of security. It’s fine to focus on your most critical firewalls initially, but you need to address the rulesets across all firewalls eventually.

Business Challenge #4: Keeping up with rules and regulations

Keeping up with the various compliance regulations, as well as business partners, customer and internal policy requirements, can be quite a challenge. You have to consider things such as:

- What's actually needed for each regulation or policy.
- What specific terms management and legal counsel have agreed to in contracts and SLAs.
- How your current firewall configurations and management practices impact what the business has committed to, or is entitled to.

In reality, if you look at all of the information security regulations such as PCI-DSS, GLBA and HIPAA, their essence is to ensure the confidentiality and integrity of sensitive information, and ensure the availability of the network and application environment. These are nothing more than best practices we've known—and implemented—for years.

The challenge today is that IT staff members are continually being pulled in different directions, and arguably are as disconnected from compliance as they've ever been. In many situations, it's to the point where IT professionals have little to no time to perform higher-level strategic work, including addressing compliance issues at the network level. Time is the scarcest resource in IT, and it's causing many IT managers and network administrators to become disconnected— then they get behind the eight ball when it comes to the compliance and the legal side of IT. Ironically, these issues are taking businesses in the exact opposite direction they should be headed. As a component of network security, firewall management suffers.


The Solution:

Given the complexities and nuances of information security regulations, policies and contracts, businesses can't afford to ignore what's required and what's at stake. Appoint yourself or someone to stay on top of the regulations affecting your business. If your business doesn't have an official compliance manager, that's all the more reason for you to stay connected with what your business must adhere to.

Ideally, you need a formal information security committee consisting of various decision-makers from HR, legal, operations, IT and internal audit. Having the right people on board will ingrain information security responsibility across the organization. It will also help ensure that all the regulations, policies and contracts to which the business is held accountable are properly communicated.

Keep in mind that the regulations your business is up against are no more than security best practices that you've likely had in place, in some capacity, before now. Plus, the various regulations are not all that different from one another. By addressing compliance from the perspective of higher-level information risk management, you can minimize security risks and adhere to all the regulations across the board.

Utilize automated tools that are both network aware (e.g., they know which network subnets are protected PCI zones) and security aware (e.g., aware of specific PCI requirements or your custom corporate policy). Such tools can assess your firewall policies against compliance regulations and flag exceptions that need attention.



Compliance can seem overwhelming, but considering what the regulators are trying to accomplish, you should be able to translate the requirements into your firewall management initiatives— especially if you have the right people and tools, and everyone is aware of what it takes to keep up.

Business Challenge #5: Proving where things stand

Keeping up A key aspect of network security is insight: having the proper visibility into your network and being able to prove your security or compliance status at any given time.

The need to prove your current security status ties directly into firewall management, rulebase maintenance and so on. We've been proving where things stand with firewalls for decades. The problem is that we haven't been doing it all that well.

There are many scenarios in which you need to know where things stand within your firewall environment, such as:

- An IT auditor needs to assess your existing controls.
- Management is looking to better understand network security.
- You suspect your network is under attack.
- A forensics investigator is analyzing a network breach that has already occurred.

Proving where things stand is the essence of compliance and general information risk management. If you can't prove where things stand at any given point in time, then what good are your firewall controls? Can you really say that you have a grasp on your overall network security? Odds are the answer is no.

The Solution:

Being able to prove your existing firewall security or compliance status requires the right controls, properly implemented. This includes technical controls such as audit logging and alerts built into your firewalls. Practically every firewall has these controls out-of-the-box, but in many cases network administrators and security managers aren't taking advantage of them.

The problem with stock solutions is that they can become unwieldy when you have more than a handful of firewalls to manage. When you have an enterprise scale deployment that includes mixture of firewall vendors, third-party firewall management applications can help take the pain away and enable greater insight into your firewall environment. Such tools can even generate out-of-the-box reports that instantly demonstrate compliance with industry regulations and corporate policies, thus saving valuable audit preparation time.



Moving Forward

Firewall management is often out of sight and out of mind. However, what may seem trivial or unimportant with firewalls can have a tremendous impact on the business if something goes awry. Never forget that IT is there for the business. Do what it takes to set up yourself, your network administrators and your business for success. Look beyond the bits and bytes to see the business tie-ins that network security and firewall management have. Ensure you're using the right tools and have reasonable processes in place that allow you to make informed network security decisions and provide value with little to no impact on the business.

You must be able to gain insight into your network, and then manage it consistently on an ongoing basis. Without the proper tools and processes, it will be difficult to claim that you have a secure and stable firewall environment that's ready to take on whatever comes your way.

About AlgoSec

AlgoSec simplifies, automates and orchestrates security policy management to enable enterprise organizations and service providers to manage security at the speed of business. Over 1,500 of the world's leading organizations, including 15 of the Fortune 50, rely on AlgoSec to optimize the network security policy throughout its lifecycle, to accelerate application delivery while ensuring security and compliance. AlgoSec is committed to the success of each and every customer, and provides the industry's only money-back guarantee.

For more information visit <http://www.AlgoSec.com> or visit our [blog](#).



Global Headquarters
65 Challenger Road,
Suite 320
Ridgefield Park
NJ 07660, USA
+1-888-358-3696

EMEA Headquarters
80 Coleman Street
London EC2R 5 BJ
United Kingdom
Tel: +44 207-099-7545

APAC Headquarters
10 Anson Road, #14-06
International Plaza
Singapore 079903
+65-3158-2120

AlgoSec.com

