algosec

AUTOMATING FIREWALL CHANGE MANAGEMENT

AN ALGOSEC WHITEPAPER

BUSINESS-DRIVEN
SECURITY MANAGEMENT

www.AlgoSec.com

INTRODUCTION

In today's IT environment, the only constant is change. Not only is change rampant, but it often occurs at breakneck speed. For a variety of reasons – rapid business growth from mergers and acquisitions, development of new applications, de-commissioning of old applications, new users, evolving networks and evolving cyberthreats – business needs change and, as they do, so must security policies.

But change comes with challenges, often leading to major headaches for IT operations and security teams. The headaches sometimes develop into huge business problems:

- Manual workflows and change management processes are time-consuming and impede IT from keeping up with the necessary business agility
- Improper management of even minor changes can lead to serious business risks as benign as blockage of legitimate traffic all the way to putting the entire network offline

Some organizations have grown so wary of change control and its potential negative impact that they resort to network freezes during peak business times rather than attempt to implement an urgent change in their network security policies.

AlgoSec has another point of view. We want to help you embrace change through process improvement, identifying areas where automation and actionable intelligence can simultaneously enhance security and business agility – without the headaches.

Herein, you will learn the secrets of how to elevate your firewall change management from manual labor-intensive work to a full automated change management process.

WHY IS IT SO HARD TO MAKE CHANGES TO NETWORK POLICIES?

Placing a sticky note on your firewall administrator's desk and expecting the change request to be performed pronto does not constitute a formal policy. Yet, shockingly, this is common practice. A formal change request process is in order. Such a process dictates clearly defined and documented steps for how a change request is to be handled, by whom, how it is addressed within a specified SLA, and more.

Using IT ticketing systems

Popular IT ticketing systems, like ServiceNow and Remedy, are a good place to manage your firewall change requests. However, these system are built for tracking general requests and were never designed for handling complex requests such as opening the network flow from server A to server B or revising user groups.

Informal change processes

Having a policy state "this is what we must do" is a start, but without a formal set of steps for carrying out and enforcing that policy, you still have a long way to go in terms of smoothing out your change processes. In fact, the majority of challenges for managing network security devices include:

- Time-consuming manual processes
- Poor change-management processes
- Error-prone processes

Firewall change management requires detailed and concise steps that everyone understands and follows. Exceptions must be approved and documented, continuously improving the process over time.

Communication breakdown

Network security and operations staff work in separate silos. Their goals, and even their languages, are different. Working in silos is a clear path to trouble. It is a major contributor to out-of-band (unexpected) changes which are notorious for resulting in "out-of-service." In many large companies, routine IT operational and administrative tasks may be handled by a team other than the one that handles security and risk-related tasks. Although both teams work toward the same goal – smooth operation of the digital side of the business – decisions and actions made by one team may lead to problems for the other. Sometimes, these situations are alleviated in a rush with the good intention of dealing with security issues "later." But this crucial "later" never comes and the network sits open to breach.

In fact, according to a large-scale survey of our own customers, out-of-process firewall changes resulted in system outages for a majority. In addition, our customers pointed out that out-of-process changes have caused them exposure to data breaches and costly audit failures.

How will you know if it's broken?

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 no-less-devastating impact of poorly managed firewall changes. Without carefully analyzing how even the most minor firewall changes are going to impact the network environment, businesses can suffer dramatic problems. Without thoughtful analysis, they might not know:

- What does the change do to vital visibility across the network?
- Which applications and connections are broken by this change?
- Which new security vulnerabilities are introduced?
- How will performance be affected?

A lot of money and effort is put into keeping the bad guys out, while we forget that "we have seen the enemy and he is us."

Network complexity is a security killer

Renowned security expert, Bruce Schneier, has stated, "Complexity is the worst enemy of security." The sheer complexity of any given network can lead to a lot of mistakes, especially when it comes to multiple firewalls with complex rule sets. Simplifying the firewall environment and management processes is necessary for good management.

DID YOU KNOW?

Up to 30 percent of implemented rule changes in large firewall infrastructures are unnecessary because the firewalls are already allowing the requested traffic!

30%

Under time pressure, firewall administrators often create more rules which turn out to be redundant with already-existing rules. This wastes valuable time and makes the firewalls even harder to manage.

MIND THE GAP? NOT IF YOU WANT A GOOD CHANGE MANAGEMENT PROCESS

Introduction of new things opens up security gaps. New hires, software patches, upgrades and network updates all increase risk exposure. The situation becomes further complicated in larger organizations which may have a mixed security estate comprising traditional, next-generation and virtualized firewalls from multiple vendors across clouds and on-premise data centers, all with hundreds of policies and thousands of rules.

Who can keep track of it all?

What about unexpected, quick-fixes that enable access to certain resources or capabilities? In many cases, a fix is made in a rush (after all, who wants a C-level exec breathing down their neck because he wants to access the network from his new tablet RIGHT NOW?) without sufficient consideration of whether that change is allowable under current security policies, or if it introduces new exposures.

Sure, you can't predict when users will make change requests, but you can certainly prepare the process for handling these requests whenever they arise. Bringing both IT operations and security teams together to prepare game plans for these situations – and for other 'knowns' such as network upgrades, change freezes, and audits – helps to minimize the risk of security gaps.

What's more, there are solutions that automate day-to-day firewall management tasks and link these changes and procedures so that they are recorded as part of the change management plan. In fact, automated technologies can help bridge the gap between change management processes and what's really taking place. They enhance accuracy, by removing people from the equation to a very large degree. For example, a sophisticated firewall and topology-aware workflow system that is able to identify redundant and unneeded change requests can increase the productivity of the IT staff.

IT operations and security groups are ultimately responsible for making sure that systems are functioning properly so that business goals are continuously met. However, these teams approach business continuity from different perspectives. The security department's number one goal is to protect the business and its data whereas the IT operations team is focused on keeping systems up and running. It is natural for these two teams to clash. However, oftentimes, IT operations and security teams align their perspectives because both have a crucial ownership stake. The business has to keep running AND it has to be secure.

But this kind of alignment of interests is easier said than done.

To achieve the alignment, organizations must re-examine current IT and security processes. Let's have a look at some examples of what happens when the alignment is not effected.

REAL-LIFE EXAMPLES OF GOOD CHANGES GONE BAD

Example 1

A classic lack of communication between IT operations and security groups put XYZ Corporation at risk. An IT department administrator, who was trying to be helpful, took the initiative to set up (on his own, with no security involvement or documentation) an FTP share for a user who needed to upload files in a hurry.

By making this change off-the-cuff, the IT admin quickly addressed the client's request and the files were uploaded. However, the FTP account lingered unsecured well beyond its effective "use by" date. By the next day, the security team noticed larger spikes of inbound traffic to the server from this very FTP account. Hackers abound. The FTP site had been compromised and was being exploited to host pirated movies.

Example 2

A core provider of e-commerce services to businesses in the U.S. suffered a horrible fate due to a simple, but poorly managed, firewall change. One day, all e-commerce transactions in and out of its network ceased and the entire business was taken offline for several hours. The costs were astronomical.

What happened?

An out-of-band (and untested) change to a core firewall broke the communication between the e-commerce application and the internet. Business activity ground to a halt.

Because of this 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 uncovered: IT staff chose not to test their firewall changes, bypassing their "burdensome" ITIL-based change management procedures. They were oblivious to the consequences.

TIPS FROM YOUR PEERS

Taken from *The Big Collection of Firewall Management Tips*

Document, document, document … And when in doubt, document some more!

"It is especially critical for people to document the rules they add or change so that other administrators know the purpose of each rule and whom to contact about it. Good documentation can make troubleshooting easy. It reduces the risk of service disruptions that inadvertently occur when an administrator deletes or changes a rule they do not understand."
— Todd, InfoSec Architect, United States

"Keep a historical change log of your firewall policy so you can return to safe harbor in case something goes wrong. A proper change log should include the reason for the change, the requester and approval records."
— Pedro Cunha, Engineer, Oni, Portugal

TAKING THE FIRE DRILL OUT OF FIREWALL CHANGES

Automation is the key. It helps staff disengage from firefighting and bouncing reactively between incidents. It helps them gain control.

The right automation solution can help teams track down potential traffic or connectivity issues and highlight areas of risk. Administrators can get a handle on the current status of policy compliance across mixed estates of traditional, next-generation and virtualized firewalls as well as hybrid on-prem and cloud estates. The solution can also automatically pinpoint the devices that may require changes and show how to create and implement those changes in the most secure way. Automation not only makes firewall change management easier and more predictable across large estates and multiple teams, but also frees staff to handle more strategic security and compliance tasks. Let the solution handle the heavy lifting and free up the staff for other things.

To ensure the proper balance of business continuity and security, look for a firewall policy management solution that:

- Measures every step of the change workflow so you can easily demonstrate that SLAs are being met
- Identifies potential bottlenecks and risks BEFORE changes are made
- Pinpoints change requests that require special attention

TIPS FROM YOUR PEERS

Taken from *The Big Collection of Firewall Management Tips*

"Perform reconciliation between change requests and actual performed changes. Looking at the unaccounted changes will always surprise you. Ensuring every change is accounted for will greatly simplify your next audit and help in day-to-day troubleshooting."
— Ron, Manager, Australia

"Have a workflow process for implementing a security rule from the user requesting change, through the approval process and implementation."
— *Gordy, Senior Network Engineer, United States*

10 STEPS TO AUTOMATING AND STANDARDIZING THE FIREWALL CHANGE-MANAGEMENT PROCESS

Here is the secret to getting network security policy change management right.

Once a request is made, a change-request process should include these steps:

1. **Clarify the change request and determine the dependencies.** Obtain all relevant information in the change request form (i.e., who is requesting the change and why).
2. **Get proper authorization for the change, matching it to specific devices and prioritizing it.** Make sure you understand the dependencies and the impact to business applications, other devices and systems, etc. This usually involves multiple stakeholders from different teams.
3. **Validate that the change is necessary.** AlgoSec research has found that up to 30% of changes are unnecessary. Weeding out redundant work can significantly improve IT operations and business agility.
4. **Perform a risk assessment.** Before approving the change, thoroughly test it and analyze the results so as not to unintentionally open up the proverbial can of worms. Does the proposed change create a new risk in the security policy? You need to know this for certain BEFORE making the change.
5. **Plan the change.** Assign resources, create and test your back-out plans, and schedule the change. Part of a good change plan involves having a backup plan in case a change goes unexpectedly wrong. This is also a good place in the process to ensure that everything is properly documented for troubleshooting or recertification purposes.
6. **Execute the change.** Backup existing configurations, prepare target device(s) and notify appropriate workgroups of any planned outage and perform the actual change.
7. **Verify correct execution to avoid outages.** Test the change, including affected systems and network traffic patterns.
8. **Audit and govern the change process.** Review the executed change and any lessons learned. Having a non-operations-related group conduct the audit provides the necessary separation of duties and ensures a documented audit trail for every change.
9. **Measure SLAs.** Establish new performance metrics and obtain a baseline measurement.
10. **Recertify policies.** While not necessary for every rule change, part of your change management process should include a review and recertification of policies at an interval that you define (e.g., once a year). Oftentimes, rules are temporary – needed only for a certain period of time – but they are left in place beyond their active date. This step forces you to review why policies are in place, enabling you to improve documentation and to remove or tweak rules to align with the business.

In some cases (e.g., data breach) a change to a firewall rule set must be made immediately, where, even with all the automation in the world, there is no time to go through the 10 steps. To address this type of situation, an emergency process should be defined and documented.

KEY CAPABILITIES TO LOOK FOR IN A FIREWALL CHANGE MANAGEMENT SOLUTION

1. Your workflow system must be firewall- and network-aware. This allows the system to gather the proper intelligence by pulling the configuration information from the firewalls to understand the current policies. Ultimately, this reduces the time it takes to complete many of the steps within the change process. In contrast, a general change management system will not have this integration and thus will provide no domain-specific expertise when it comes to making firewall rule changes.
2. Your solution must support all of the firewalls and routers used within your organization. With the evolution of next-generation firewalls and new cloud devices, you should also consider how your plans fit into your firewall change-management decisions. In larger organizations, there are typically many firewalls from different vendors. If your solution cannot support the all of the devices in the environment (current and future), then this isn't the solution for you!
3. Your solution must be topology-aware. The solution must:
   - Understand how the network is laid out
   - Comprehend how the devices fit and interact
   - Provide the necessary visibility of how traffic is flowing through the network
4. Your solution must integrate with the existing general change management systems. This is important so that you can maximize the return on previously made investments. You don't want to undergo a massive retraining on processes and systems simply because you have introduced a new solution. This integration allows users to continue using their familiar systems, but with the added intelligence from having that firewall-aware visibility and understanding that the new solution delivers.
5. Your solution must provide out-of-the-box change workflows to streamline change-management processes as well as be highly customizable since no two organizations' network and change processes are exactly the same. Key workflow capabilities to look for in a solution:
   - Provide out-of-the-box change workflows to help you quickly tackle common change-request scenarios
   - Offer the ability to tailor the change process to your unique business needs by:
     - Creating request templates that define the information required to start a change process and pre-populate information where possible
     - Enabling parallel approval steps within the workflow — ideal when multiple approvals are required to process a change
     - Influencing the workflow according to dynamic information obtained during ticket processing (e.g., risk level, affected firewalls, urgency, etc.)
     - Ensuring accountability and increasing corporate governance with logic that routes change requests to specific roles throughout the workflow
   - Identify which firewalls and rules block requested traffic
   - Detect and filter unneeded/redundant requests for traffic that is already permitted
   - Provide "what-if" risk- analysis to ensure compliance with regulations and policies
   - Automatically produce detailed work orders, indicating which new or existing rules to add or edit and which objects to create or reuse
   - Prevent unauthorized changes by automatically matching detected policy changes with request tickets and reporting on mismatches
   - Ensure that change requests have actually been implemented on the network, preventing premature closing of tickets.

OUT-OF-THE-BOX WORKFLOW EXAMPLES

The best solutions allow for:

- Adding new rules via a wizard-driven request process and flow that includes impact analysis, change validation and audit
- Changing rules and objects by easily defining the requests for creation, modification and deletion, and identify rules affected by suggested object modifications for best impact analysis
- Removing rules by automatically retrieving a list of change requests related to the rule-removal request, notify all requestors of the impending change, manage approval process, document and validate removal
- Recertifying rules by automatically presenting all tickets with deadlines to the responsible party for recertification or rejection and maintaining a full audit trail with actionable reporting
- Quantifying the ROI on firewall change-control automation

CUT YOUR COSTS

Manual firewall change management is a time-consuming and error-prone process. Consider a typical change order that requires a total of four hours of work by several team members during the change lifecycle, including communication, validation, risk assessment, planning and design, execution, verification, documentation, auditing and measurement.

Based on these assumptions, AlgoSec customers have reported significant cost savings (as much as 60%) achieved through:

- Reduction of 50% in processing time using automation
- Elimination of 30% of unnecessary changes
- Elimination of 8% of changes that are reopened due to incorrect implementation

SUMMARY

While change management is complex stuff, the decision for your business is actually simple. You can continue to slowly chug along with manual change management processes that drain your IT resources and impede agility. Or you can accelerate your processes with an automated network change-management workflow solution that aligns the different stakeholders involved in the process (network operations, network security, compliance, business owners, etc.) and helps the business run more smoothly.

Think of your change process as a key component of the engine of an expensive car (in this case, your organization). Would you drive your car at high speed if you didn't have tested, dependable brakes or a steering wheel? Hopefully, the answer is no! The brakes and steering wheel are analogous to change controls and processes. Rather than slowing you down, they actually make you go faster, securely! Power steering and power brakes (in this case firewall-aware integration and automation) help you zoom to success.

ABOUT ALGOSEC

The leading provider of business-driven security management solutions, AlgoSec helps the world's largest organizations align security with their business processes. With AlgoSec, users can discover, map and migrate business-application connectivity, proactively analyze risk from the business perspective, tie cyber-attacks to business processes and intelligently automate network-security changes with zero touch — across their cloud, SDN and on-premise networks. Over 1,500 enterprises, including 20 of the Fortune 50, utilize AlgoSec's solutions to make their organizations more agile, more secure and more compliant. Since its inception, AlgoSec has offered the industry's only money-back guarantee.