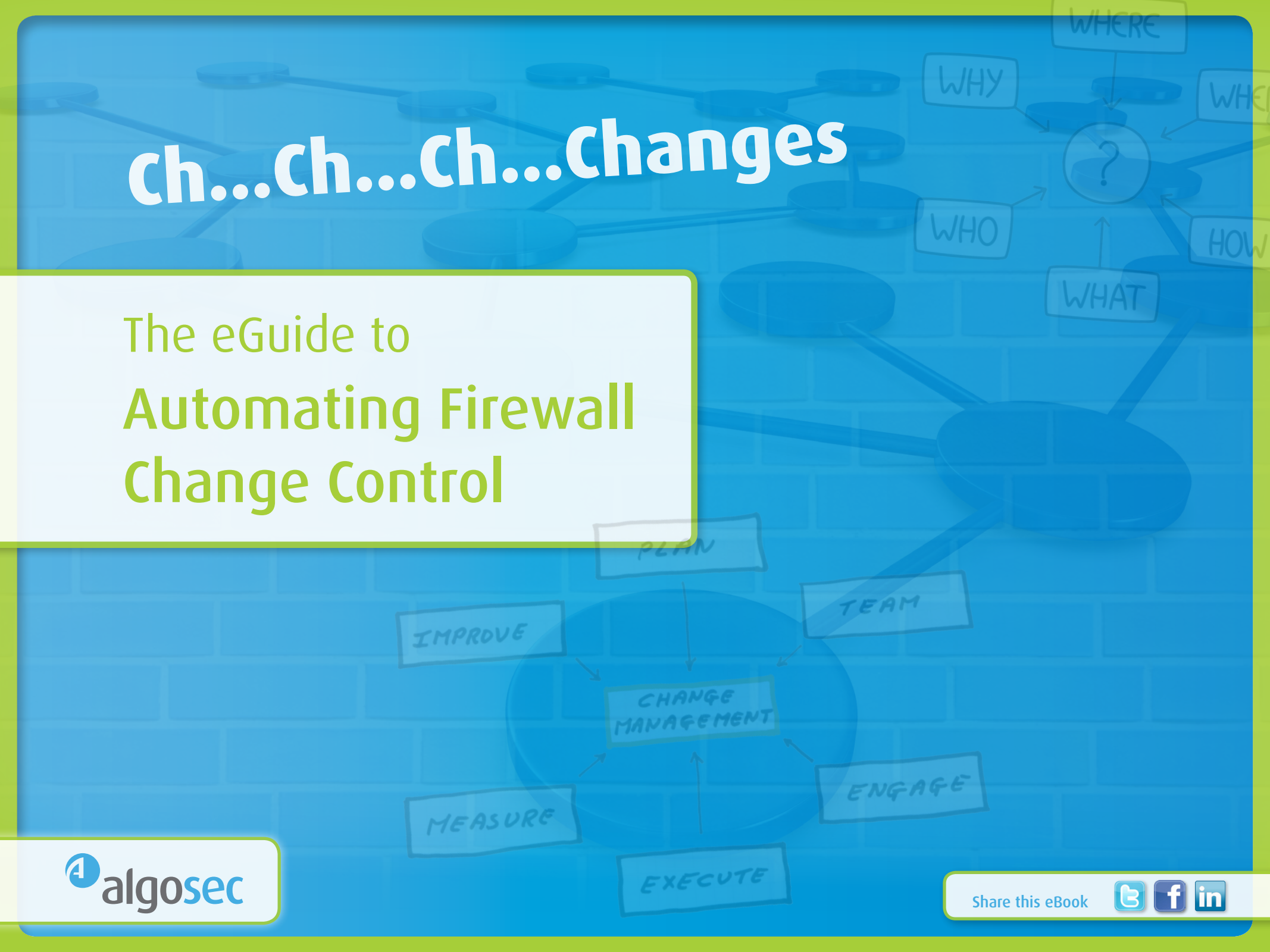
Ch...Ch...Ch...Changes

The eGuide to
Automating Firewall Change Control



algosec

Share this eBook

Change.

The only thing that stays the same in today's IT environment is that there is always change. Not only is it common, but change often occurs at a breakneck pace. As business needs change (due to rapid business growth from mergers and acquisitions, new applications being spun up, old applications being decommissioned, new users, evolving networks and new threats), so must security policies.

All of this can lead to major headaches for both IT operations and security teams and become a huge business problem:

- Manual workflows and change management processes are time-consuming and impede IT agility.
- Improper management of 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.
- Some organizations are so concerned about change control and its potential negative impact that they even resort to network freezes during peak business times.

We've developed this eGuide to help you (YOU should be an IT security and/or operations professional) embrace change through process improvement and identification of areas where automation and actionable intelligence can enhance both security AND business agility.

By continuing on this journey with us, you will learn how to take your firewall change management

From...

To

Inside this Ebook

What Makes Change So Tough?

Before we dig into the "how" when it comes to automating firewall change management, let's first step back and level set on the "why," as in why change can be so daunting. From an IT perspective, change means work... and potentially a lot of it. And with IT organizations stressed to the max, there are many factors that contribute to problems with firewall change management.

Post-it Note Policies

Placing a sticky note on your firewall administrator's desk and expecting the change request to be performed does not constitute a formal policy! Yet shockingly this is commonplace. A formal change request process includes clearly defined and documented steps for how a change request will be handled, by whom, addressed within a specified SLA, etc.

Informal Change Processes

Having a policy state "this is what we must do" is a good first step, but without a formal set of steps for carrying out and enforcing that policy, you still have a ways to go in terms of solidifying your change processes. The majority of challenges (55.6%) 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 follows when changes are needed. Any exceptions need to be approved and documented.

Source: The State of Network Security 2012, April 2012

The Dangers of the Holiday Freeze

Guest Blog by Matthew Pascucci, Information Security Writer and Practitioner

During the Christmas holiday season many companies utilize network freezes to protect themselves from errant changes which could cause outages during valuable high traffic days. Many companies put these freezes into effect to prevent business disruption — and potentially lost business - and are generally good ideas. But by protecting the organization could we really be putting ourselves at risk? To freeze for the sake of freezing can cause a company to stay frozen in a vulnerable, unprotected state...

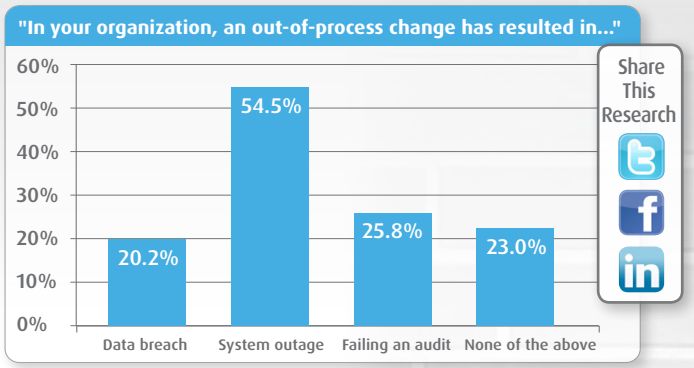
Read the rest of this blog

What Makes Change So Tough?

Communication Breakdown

Network security and operations staff working in silos is a clear path to trouble and a major contributor to out-of-band changes, which typically result in "out-of-service." In many larger companies, routine IT operational and administrative tasks may be handled by a different team than the one that handles security and risk-related tasks. Although both teams are working toward the same end, decisions made by one team may lead to issues for the other. Sometimes these situations can be dealt with in a rush, with the full intention of dealing with any security issues afterward. But this latter, crucial element may get overlooked.

Out-of-process firewall changes resulted in system outages for a majority (54.5%) of the organizations surveyed. For 77.0% of respondents, out-of-process changes caused a system outage, a data breach, an audit failure, or more than one of these serious problems.



Source: The State of Network Security 2012, April 2012

If It's Broke How Will You Know?

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. Not analyzing and thinking through how even the most minute 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 do your changes break?
- Which new security vulnerabilities are going to be introduced?
- How will performance and visibility be affected?

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.

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 your firewall environment and management processes is a must.

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!

Unfortunately, without the proper solution it is very difficult to determine whether a change is necessary.

So, more often than not, firewall administrators simply create more (redundant) rules. This wastes valuable time and, in the process, makes the firewalls even harder to manage.

Mind the Gap? Not if You Want a Good Change Management Process

Change management formalizes the way we work and how to document the "who, what, when, why and how" of all firewall changes.

Every new hire, every software patch or upgrade, and every network update opens up a security gap and increases the organization's risk exposure. This situation becomes further complicated in larger organizations, which may have a mixed security estate comprising traditional, next-generation and virtualized firewalls from multiple vendors, all with hundreds of policies and thousands of rules.

Then there are unexpected, quick-fix changes for access to specific resources or capabilities. In some cases, the change 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 exposure to risk.

You can't always predict when users will make change requests, but you can certainly prepare a routine for handling these requests when 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 these changes causing security holes.

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 and remove people from the equation to a great extent. 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 your IT staff.

Why operations and security don't mix — and why they should

By Dr. Avishai Wool,
AlgoSec CTO and Co-Founder

IT operations and security groups are ultimately responsible for making sure an organization's systems are functioning so that business goals are met. However these teams approach business continuity from different perspectives. The security department's number one goal is to protect the company, whereas the IT operations team is focused on keeping systems up and running. Oftentimes, IT operations and security teams must work together and be on the same page because both have an ownership stake. This is easier said than done.

To achieve this alignment, organizations must re-examine current IT and security processes and...

Read more at Last Watchdog

Real-Life Examples of Changes Gone Bad

Change can be good. But if not managed properly, change can open up a can of worms when it comes to your security. Here are two examples of changes gone bad:

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

   Through this change, the IT admin quickly addressed the client's request and the files were uploaded. However... the FTP account was left up and unsecured and by the next day, the security team noticed larger spikes of inbound traffic to the server with this FTP account. The FTP site had been compromised and was being used to host pirated movies.

2. A core provider of e-commerce services to businesses in the U.S. suffered a worse fate due to a 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. Some out-of-band (and untested) changes to a core firewall broke the communication between the e-commerce 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.

For more real-life firewall changes gone bad, read Network Security Horror Stories: Change Control by infosecurity practitioner Matthew Pascucci.

Tips from Your Peers
(taken from **The Big Collection of Firewall Management Tips**)

Document, Document, Document...

"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 who to contact about them. Good documentation can make troubleshooting easy and reduces the risk of service disruptions that can be caused 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

> "The best way to manage network security operations is to link security and operations through change management and change control, and to supplement and accelerate automation."
>
> *— Greg Young, Research VP, Gartner*

Automation helps staff move away from firefighting and being bounced reactively between incidents, and helps them gain control. The right solution can help teams track down potential traffic or connectivity issues, highlights areas of risk, and the current status of compliance with policies across mixed estates of traditional, next-generation and virtualized firewalls. It can also automatically pinpoint the exact devices that may need changes, and show how to design and implement that change in the most secure way.

This 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, because the solution is handling much of the heavy lifting.

Watch this video to hear how BT has automated their firewall change management process.

Share this video

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 SLAs are being met,
- identifies potential bottlenecks and risks — before changes are made, and
- pinpoints change requests that require special attention.

Tips from Your Peers
(taken from The Big Collection of Firewall Management Tips)

Accountability between requests and actual changes...

"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."

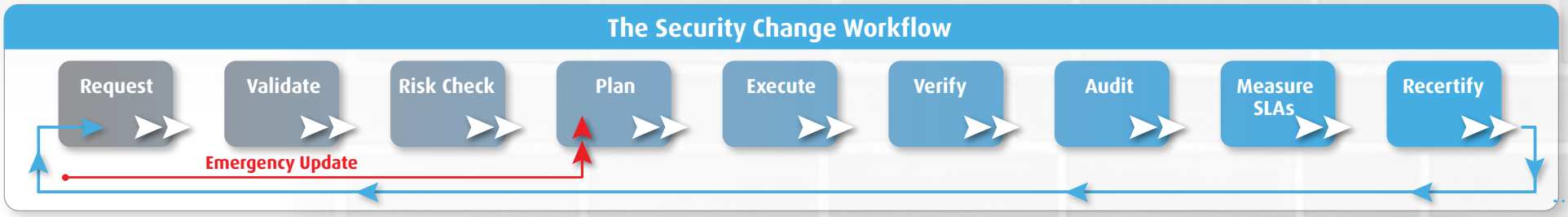
Gordy, Senior Network Engineer, United States

The Ideal Firewall Change Management Process

A typical change request process may include the following steps once the request has been made:

1. **Clarify the user request and determine dependencies.** Obtain all relevant information in the change request form (i.e. who is requesting the change and why), get proper authorization for the change, match the change to specific devices, and prioritize the change. Make sure you understand the dependencies and the impact to business applications, other devices and systems, etc. which usually involves multiple stakeholders from different teams depending on the foreseen impact.
2. **Validate that the change is needed.** AlgoSec research has found that up to 30% of changes are unnecessary, thus weeding out this redundant work can significantly improve IT operations and business agility.
3. **Perform a risk assessment.** Thoroughly test the change and analyze the results before approving the change, so as not to unintentionally open up a can of worms. Does a proposed change create a new risk in the security policy? You want to know this BEFORE making the change.
4. **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 bad. This is also a good place in the process to ensure that everything is properly documented for troubleshooting or recertification purposes.
5. **Execute the change.** Backup existing configurations, prepare the target device, notify appropriate workgroups of any planned outage, and perform the actual change.
6. **Verify correct execution to avoid outages.** Test the change, including affected systems and network traffic patterns.
7. **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 documentation trail for every change.
8. **Measure SLAs.** Establish new performance metrics and obtain a baseline measurement.
9. **Recertify policies.** While not necessary for every rule change, it should be a part of your change management process at an interval that you define (i.e. once a year, twice a year, etc.) to review and recertify policies. Oftentimes there are rules only needed for a period of time, but left in place beyond their intent. This step forces you to review why policies are in place, to improve documentation, and to remove or tweak rules to align with the business.

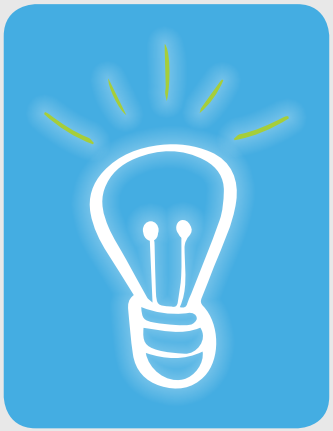
In some cases (i.e. data breach) a change to the firewall rule set must be made immediately, where even with all the automation in the world, there is no time to go through all of the above steps. To address this type of situation, an emergency process should be defined and documented.



Key Capabilities to Look for in a Firewall Change Management Solution

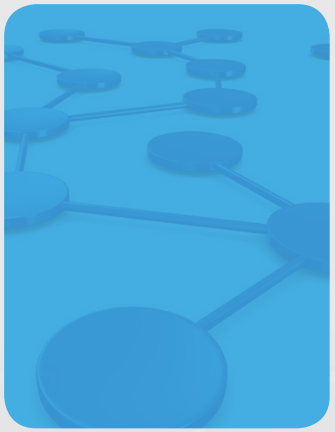
There are several baseline requirements when selecting a firewall change management solution that you should make sure are on your checklist.

1. **Your workflow system must be firewall-aware.** This allows the system to gather the proper intelligence, by pulling the configuration information from the firewalls to understand the current policies and ultimately reduce the time it takes to complete many of the critical steps within a 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.

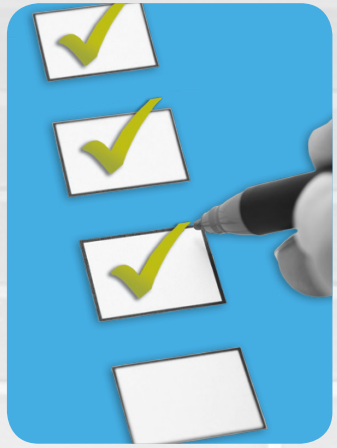


2. **Your system must support all of the firewalls and routers used within your organization.** With the evolution of next-generation firewalls, you should also consider your plans here and how that fits into you firewall change management decisions. In larger organizations there are typically many firewalls from different vendors and if your solution cannot support the current and or potential future devices in the environment, then it isn't the solution for you!

3. **Your solution must be topology-aware.** This means that the solution must:
   - Understand how the network is laid out
   - Understand the devices fit and interact
   - Provide the necessary visibility of how traffic is flowing through the network



4. **Your system must integrate with existing general change management systems.** This is important so that you can maximize the return on previously made investments. What you don't want to have happen is to require massive retraining of process and systems because now there is a new system to manage. This integration allows users to continue using the software they are used to, but with the added intelligence having that firewall-aware visibility and understanding.



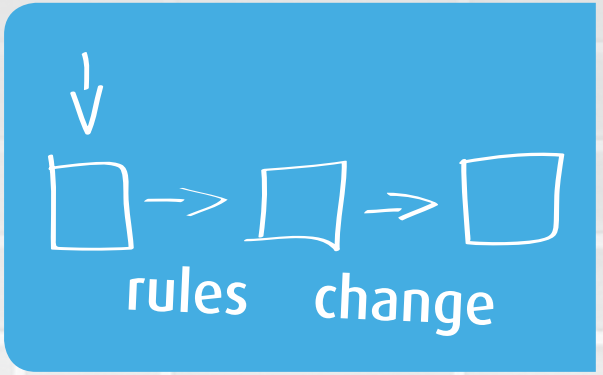
Continued...

Key Capabilities to Look for in a Firewall Change Management Solution

5. Your system must provide out-of-the-box change workflows to streamline the process as well as be highly customizable — as no organization's network and change processes are exactly the same.

Key workflow capabilities to look for a solution:

- ✓ Provide out-of-the-box change workflows to help you quickly tackle common change request scenarios
- ✓ Provide the ability to tailor the change process to your unique business needs
  - Create request templates that define the information required to start a change process and pre-populate information where possible.
  - Enable parallel approval steps within the workflow — ideal for when multiple approvals are required to process a change.
  - Influence the workflow according to dynamic information obtained during ticket processing (i.e. risk level, affected firewalls, urgency, etc.).
  - Ensure accountability and increase corporate governance with logic that routes change requests to specific roles in the workflow.
- ✓ Identify which firewalls and which rules block the requested traffic.
- ✓ Detect and filter unneeded/redundant requests for traffic that is already permitted.
- ✓ Provide "what-if" risk-check analyses 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 report on mismatches.
- ✓ Ensure that change requests have actually been implemented on the network, preventing premature closing of tickets.



Out-of-the-Box Workflows for Real Life Scenarios

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 the 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.

Ch-Change... Ch-Ching: Quantifying the ROI on Firewall Change Control Automation

As we've examined, manual firewall change management is a time-consuming and error-prone process. Automating this process can result in significant and measurable savings for an enterprise (see the following table).

Consider a typical change order that requires a total of four hours of work by all team members throughout the change life cycle, including communication, validation, risk assessment, planning and design, execution, verification, documentation, auditing and measurement. The "loaded" cost per working hour of the IT staff involved in the change process is $60.

Based on these assumptions, AlgoSec customers have reported significant cost savings of up to 60 percent, achieved through:

- ✓ Reduction of 50 percent in processing time using automation
- ✓ Elimination of 20 to 30 percent of unneeded changes
- ✓ Elimination of 2 to 8 percent of changes reopened due to incorrect implementation

Annual Changes	Working Hours	Annual Cost ($)	Annual Savings ($)
500	2,000	$120,000	$72,000
2,000	8,000	$480,000	$288,000
5,000	20,000	$1,200,000	$720,000

Now that puts the "ch-ching" into "change"!

Conclusion

While change management is complex stuff, the decision for your business is actually fairly simple. You could continue to slowly chug along with manual change management processes that drain your IT resources and impede agility. Or you could amp it up with an automated workflow system that helps align the different stakeholders involved in the change process (i.e. network operations, network security, compliance, business owners, etc.) and ultimately 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 any speed if you didn't have brakes? Hopefully the answer is no! The brakes and steering wheel are analogous to change controls and processes. Rather than slowing you down, they can actually make you go faster! Power steering and power brakes (in this case firewall-aware integration and automation) further help you put the pedal to the metal.