The Big Collection Of

FIREWALL MANAGEMENT TIPS

Brought to you by AlgoSec

algosec

About This eBook

Firewalls continue to serve as the first line of defense for preventing network attacks, but they also introduce the most management challenges. In a recent "**Network Security Management Attitudes**" survey, firewalls were cited as requiring the biggest time investment (64.5% of respondents) and causing the most network outages (40.8%) compared to other security technologies such as IPS/IDS, DLP and Anti-Virus.

But Firewalls are administered by very capable security professionals, who develop and utilize best practices, processes and tools to rise up to the challenge. This eBook compiles firewall management tips from real security practitioners who readily shared their expertise. We hope you will find the tips useful in your quest to protect your organization's data.

The AlgoSec Team.

algosec

Policy Management

algosec

"Manage the lifecycle of the policy by enforcing an expiration date. Normally when we set up a new service, it requires new rules on the firewall, but when the service is modified or terminated no one asks for the removal of the associated rules. By requiring the duration of the rule, we can reach out to the requestor close the deadline and ask if we need to extend the lifetime of the rule or cancel it."

Gionata, Manager, Italy

"Use the same rule set for similar policies. E.g. Production and DR can be the same policy with the same group object. The main objective is to have a simpler but global policy."

Luis, DSI, Portugal

algosec

"Don't nest object groups to simplify and clean Firewall rule management, follow the KISS (Keep it Simple Stupid) method."

Danny Sutantyo, Security Compliance Manager, Loblaw Companies Ltd, Canada

"One of the things people like to do the least is also one of the most useful things they can do and that is to DOCUMENT the changes they make to a system. With firewalls, 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. Trying to troubleshoot an issue with a firewall that has scores of undocumented rules can be very frustrating. 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

algosec

"The single most important aspect of sound firewalling, is naming conventions. Ensure all objects and rules follow these conventions."

Don Keeber, Principal Security Architect, Modcomp Systems, United States

"When you create temporary rules, make sure to add a comment with the expiration date, and regularly review expired rules."

Luis, Security Architect, Colombia

"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. These logs also help keep track of all changes made and why they have occurred."

Pedro Cunha, Engineer, Oni, Portugal

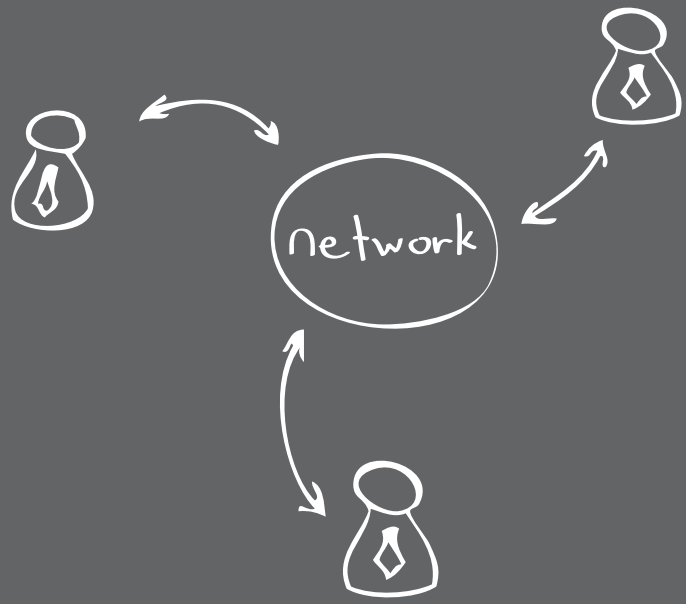
algosec

"Deny policies at the end of your rule set help make sure you catch traffic that's trying to go to the wrong zone, so it is important to have every combination covered.
Make sure you have enough deny policies between your zones with this factorial math equation: (number of zones)! / (number of zones -2)! = (number of possible two-way combinations). 3 zones with deny policies each way would mean you need 6 policies - 3! / 1! = 6. 10 zones means you need 90 unique policies - 10! / 8! = 90."

Matt
Sr. Systems Engineer
United States

"Use all available options for documentation. Group rules that belong together. Use the same naming on your firewall as you have on your clients/servers.
Try to create groups of hosts, networks or services when possible and use the groups instead of adding single objects."

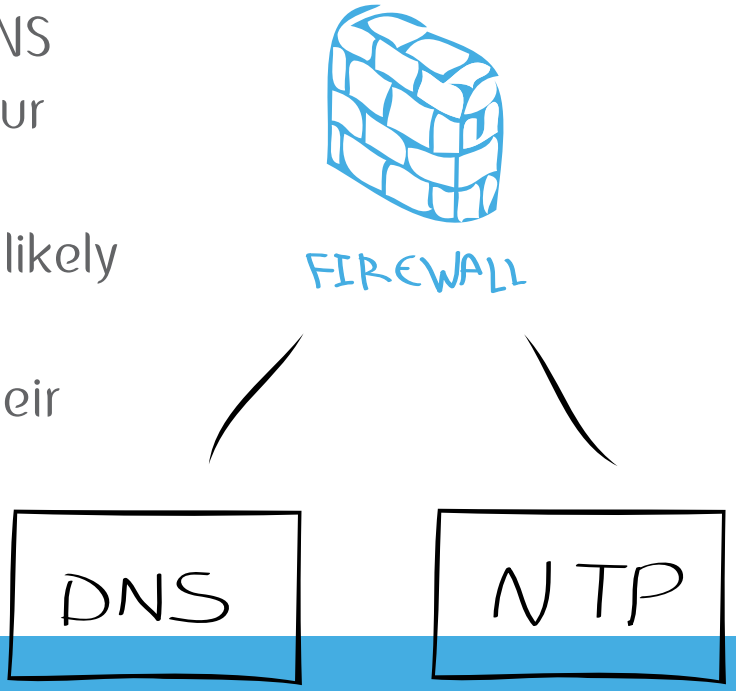
Reinhard Stich
Head of Support
Internet Security AG
Austria



algosec

"If you need to allow internal clients access to public DNS and NTP servers (or any other protocol that matches your environment), make sure you limit these connections to known trusted DNS and NTP hosts. Otherwise, you are likely to open up remote access to select employees who are using these benign protocols to tunnel their traffic via their own servers or public tunnel services on the Internet."

Vasilis, Senior Security Engineer, United States



"Always enable logging on Permit/Deny rules. This helps you to:

- Have evidence in case of an intrusion
- Troubleshoot routing (i.e.: asymmetric routing)
- Troubleshoot application communication matrix
- Make the best use of automated tools such as AlgoSec for optimization and analysis based on historical traffic."

Enrico Sorge, Senior Security Consultant, Italtel, Italy

algosec

"End your rule base with a clean-up rule or a ANY ANY DENY rule."

Justin, Senior Professional, Trinidad and Tobago

"Most Firewalls have an option to show the traffic counters against each rule. These are very beneficial both for firewall management and troubleshooting. Have a detailed look into the counters and reorder rules, placing the most used rules (the ones with the most hits) at the top.
For large rule sets, this will significantly reduce the processing load on the firewall."

Ramani Gogoi, IT Manager, OnMobile Global, India

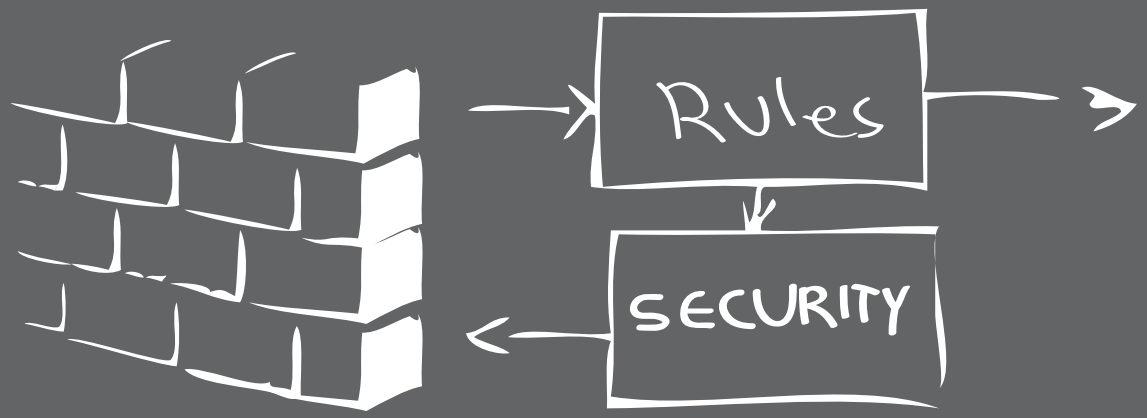
"Create a rule before the last rule that blocks broadcasting without logging. It resolves huge logging issues in firewall management."

David, Manager, Israel

algosec

"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."

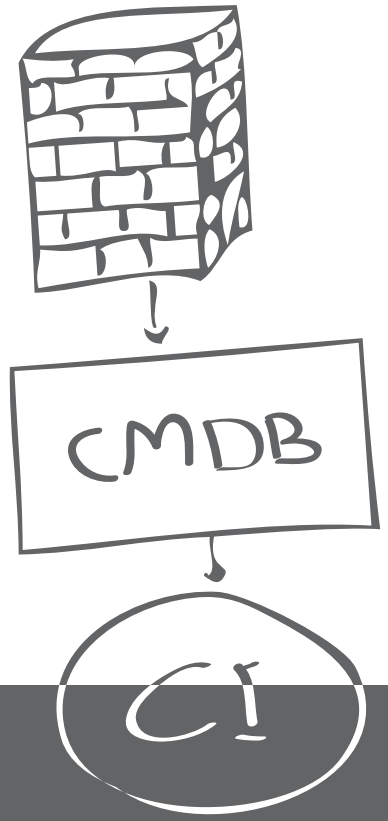
Ron, Manager, Australia



"Establish a mandatory process for periodic firewalls rules review and leverage the power of firewall analyzers to provide various types of security reports."

Piotr, Group IS Service Manager, Poland

algosec



"Use the comment field in rules and objects for enhanced functionality. For example, you can place a validity date for each object to make an easy review of the object base or make a connection to your CMDB by defining a CI reference in the object or rule."

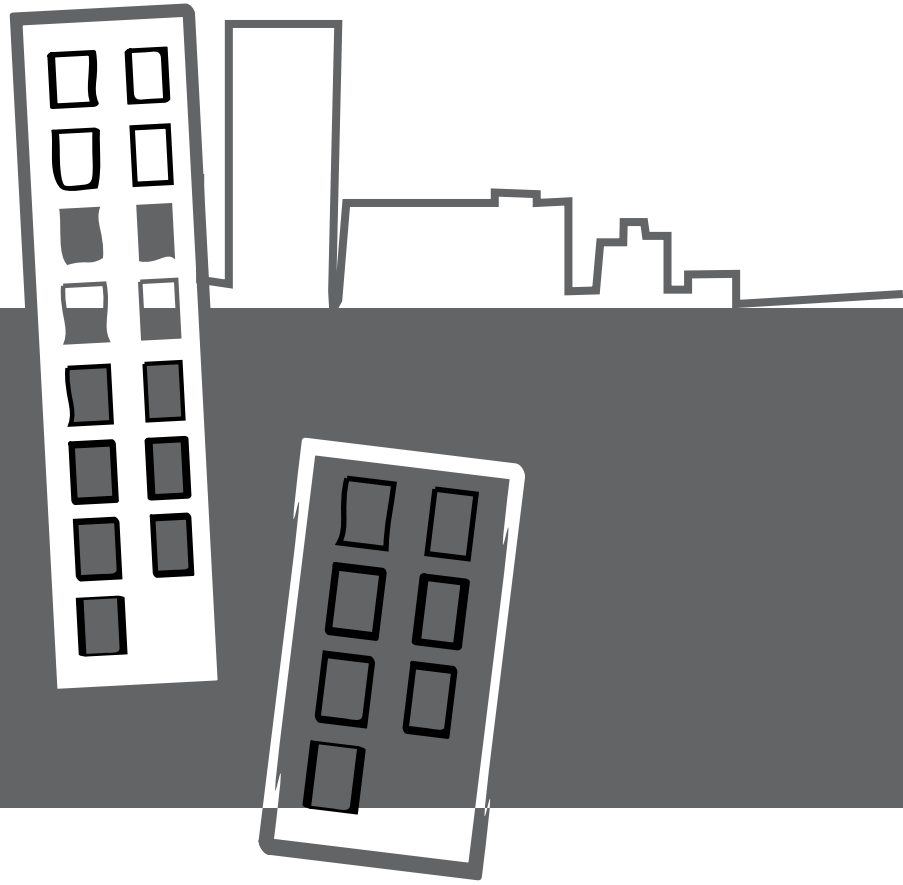
Markus, Consultant, Germany

"Document, document, document! Document all firewall rules with well-defined comments for each rule. Though it may look insignificant in day-to-day operations, it is a real lifesaver in times of crisis. Even better, use a firewall management tool which maintains a well-defined configuration database with versioning against each configuration change."

Ramani Gogoi, IT Manager, OnMobile Global, India

algosec

Architechure



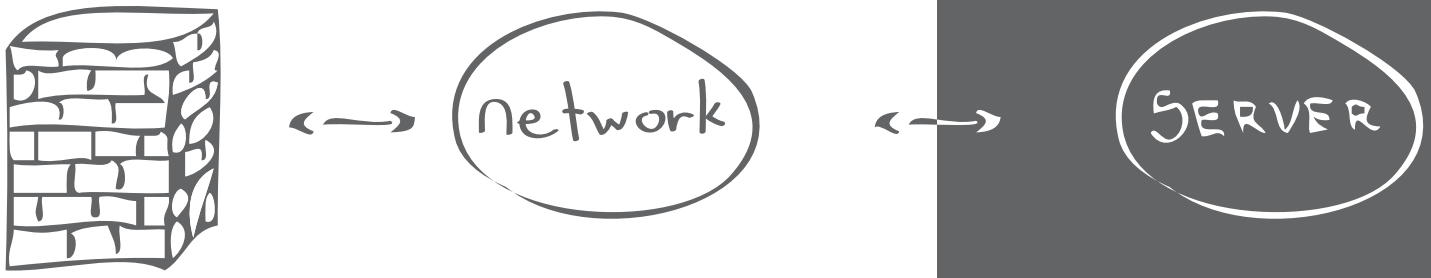
algosec

"Create physically separate networks according to the importance of the business functions performed over those networks.
Create custom-tailored firewall rules according to those functions and importance levels."

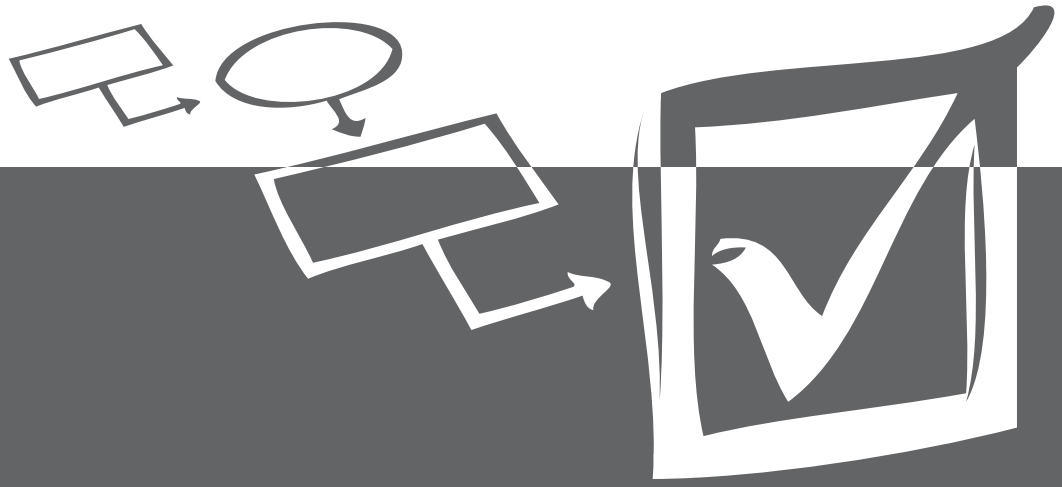
Michael, Principal, United States

"Build two networks - one for normal operations and another for management purposes (administrators may administer servers and switches from home after business hours.)
Get an Internet connection for these networks from two different ISPs.
So when an attacker tries to break your normal Internet connection, administrators have access to servers and switches via the management network."

Ahti, Software Specialist, Finland



algosec



Processes

algosec

"Keep it simple by reducing the number and type of firewalls that you need to manage. Standardize your firewall policies based on risk. Use centralized management and monitoring tools. Ensure that you have a properly trained and dedicated staff. Stay vigilant – regardless of the shiny new security technologies developed over the past 20 years, firewalls are still the gateways into and out of your network. Defend your house."

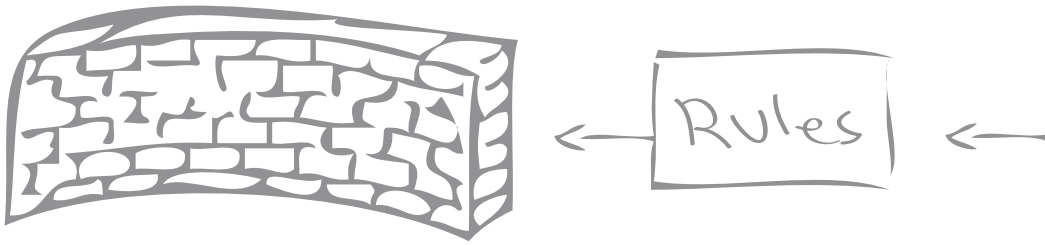
Philip Agcaoili
Chief Information Security Officer
Cox Communications
United States

"Always create Database Revision Controls. These things will save your life and give you job security! You never know when you might have to revert back to an older policy."

Fred, Security Advisor, Canada

"Define a dedicated scheme where to configure what kind of access. For instance general rules for all users, location related rules, rules for groups of users/IPs and then single user/IP rules."

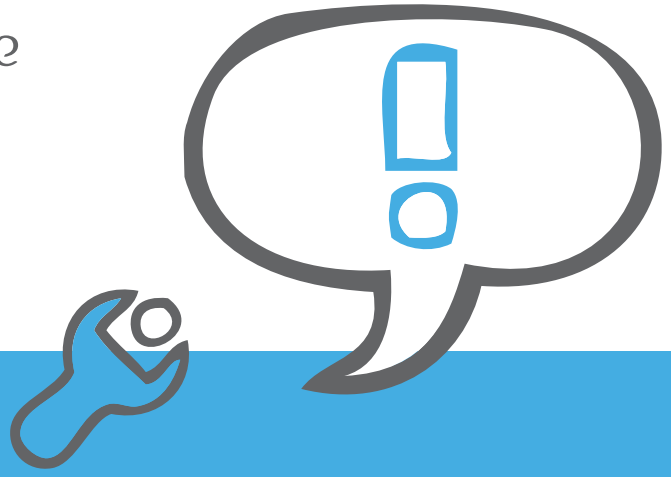
Thomas, Manager, Germany



algosec

"Never assume any firewall configuration is secure just because it's managed by an outside firm. Always include firewall review as a deliverable."

Jason Wiegand, Security Analyst, Haizlett & Associates, USA



"To ensure survivability after a disaster, ensure that backup best practices are implemented. This includes the following:

1. Periodic backup of the firewall, at least on a monthly basis. The best way to achieve this is to use the product's scheduling function (i.e. Check Point's backup command) and schedule a command to display the configuration (i.e. Cisco's show run)
2. Backup the firewall before and after making a change
3. Ensure that the backup config is usable. The backup config should be tested at least once every two years
4. Backup data should not be stored in the same location as the firewall."

Z, Security Architect, Australia

algosec

"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 firewall is always the first place fingers are pointed at when applications do not work as expected. Often a lot of time is spent speculating or negotiating whether the source of the issue is the firewall or not.
My tip is to take a look. A packet sniffer is almost always a quicker path to finding out what is happening to traffic flow than guessing and making adjustments based on those guesses. I see many engineers reluctant to fire up tcpdump, whereas it has become one of my first troubleshooting tools to bring to bear on an issue."

Paul Murphy, Security Consultant, Hum Consulting, United States

algosec

"Always analyze the risk that changes to the firewall can introduce. Make sure that the rule is implemented in the exact way that it was approved to avoid security holes. That's why I will always recommend automated tools such as Algosec for firewall management."

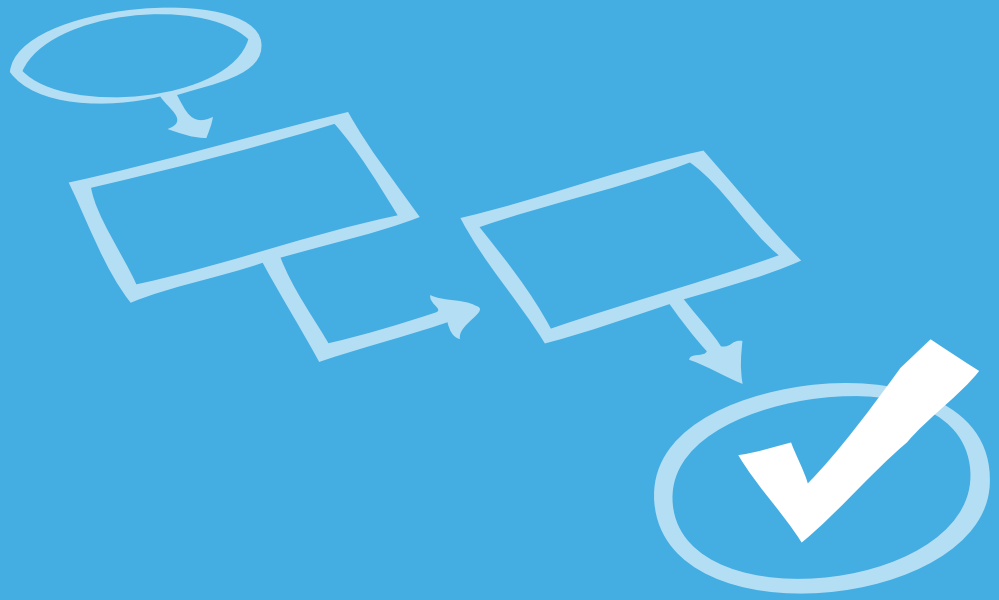
Fabrice, Security Engineer, Belgium

"Implement a robust and dynamic change management policy as soon as talks about purchasing a firewall are mentioned."

Rich, Principal, United States

"A lot of firewall policies are really grown over time. By using a firewall policy management tool we can clean up the policy and ensure a readable policy that addresses real needs. This greatly simplifies our day to day work."

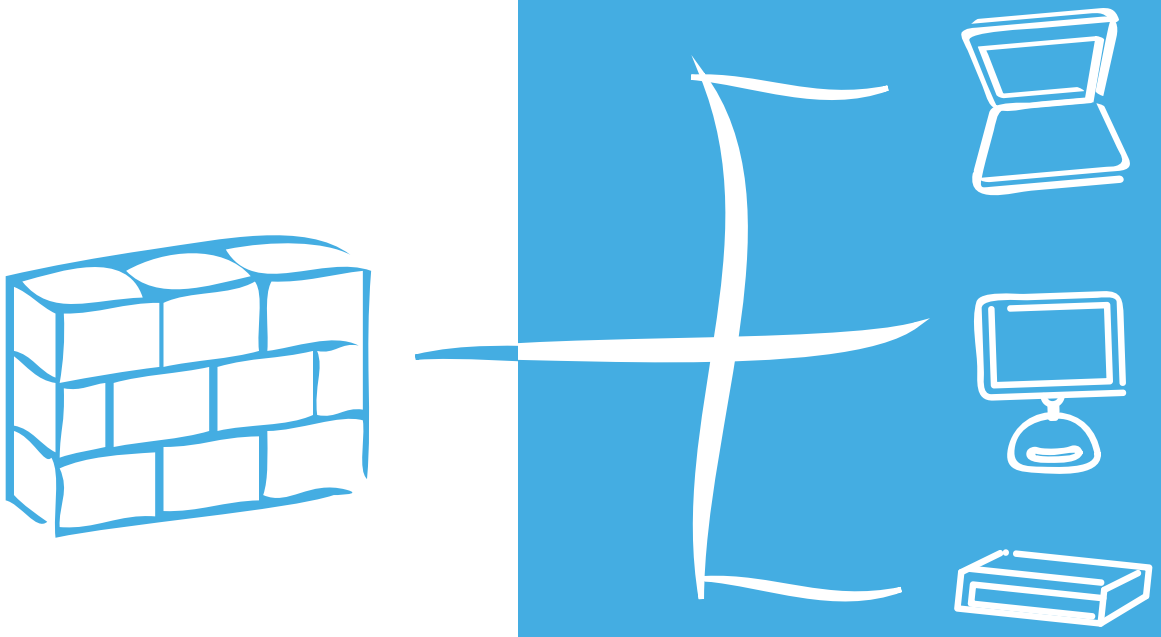
Filip D'hondt, Electrabel, Belgium



algosec

Edward Cwiklinski
Security Engineer
Walmart
United States

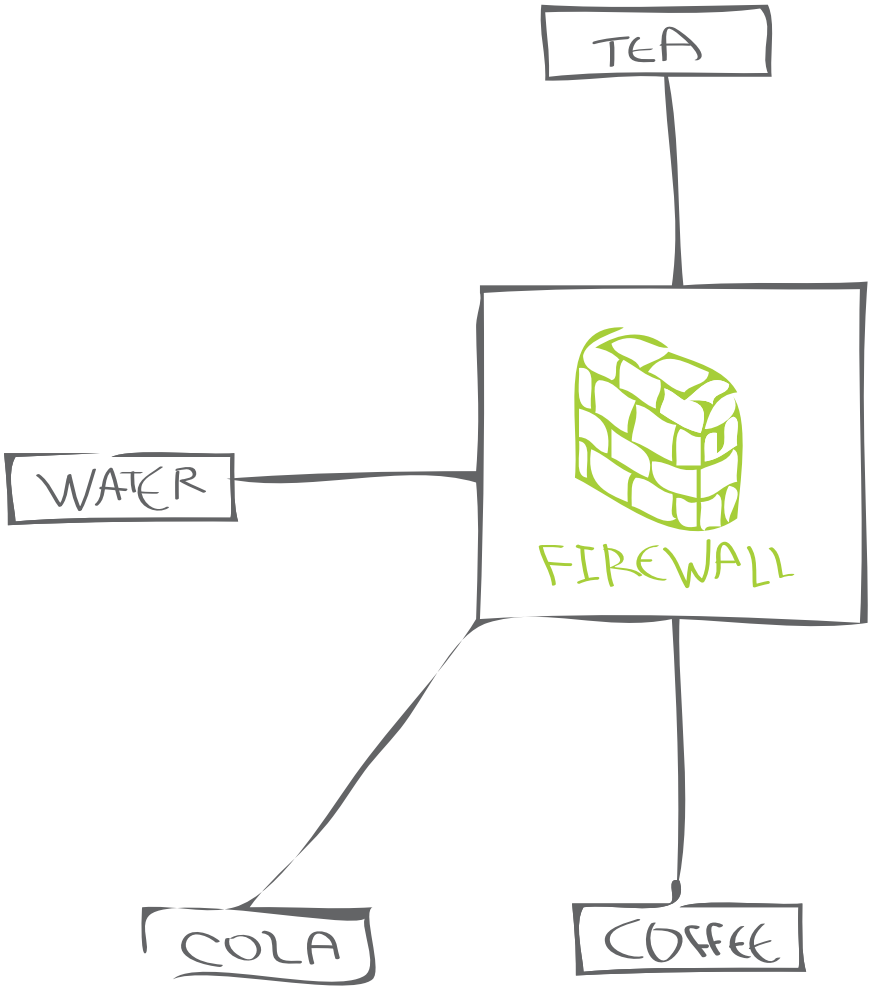
"Have an automatic process to back-up your firewall configurations to a secure location on an interval that makes sense for your environment."



algosec

Just for Laughs

algosec



"Never pour water on your firewall unless it's really on fire."

Kevin, Senior Manager, United States.

"Cleaning up your rules before Christmas makes it easier to maintain a secure ruleset throughout the year!."

Richard, Consultant, Norway

algosec

About AlgoSec

AlgoSec helps more than 700 of the world's leading organizations manage complex policies of firewalls, routers, VPNs and related security infrastructure, improving overall security while reducing operational costs.
Consisting of **AlgoSec Firewall Analyzer** and **FireFlow**, the AlgoSec Security Management Suite automates labor-intensive tasks traditionally associated with firewall operations, change management, auditing, compliance and risk analysis to ensure devices are properly configured.

For more information visit **www.algosec.com** or visit our blog "**Playing with Fire**"

Follow Us: 

algosec