

CASE STUDY

ENERGY SUPPLIER KEEPS THE LIGHTS ON WITH AUTOMATED NETWORK CHANGE MANAGEMENT

Large energy supplier empowers internal stakeholders and streamlines network security policy change process.

LINE OF BUSINESS

Utilities and Energy

LOCATION

International

The company is the provider of electricity and gas for their country. They are responsible for the planning, construction, operation, maintenance and global technical management of both these grids and associated infrastructures.

THE CHALLENGE

In order to provide power to millions of people, the company runs more than twenty IT and OT firewalls from multiple vendors that are hosted in multiple data centers throughout the country.

Some of the challenges included:

Lack of visibility over a complex architecture – With multiple networks, IT managers needed to know which network is behind which firewall and connect traffic flows to firewall rules. Change management processes were being managed by network diagrams created in Microsoft Visio and Microsoft Excel spreadsheets – tools that were not designed for network security policy management.

Thousands of rules – Each firewall may have thousands of rules each. Many of these rules are unneeded and introduce unnecessary risk. Managing the maze of rules was time consuming and took time away from other strategic initiatives.

Unnecessary requests – Business stakeholders were requesting status information about network traffic and making duplicate and unnecessary change requests for items covered by existing rules.

THE SOLUTION

The company was searching for a solution that provided:

- Visibility into their network topology, including traffic flows.
- Optimization of their firewall rules.
- Alerts before time-based rules expire.
- Automatic implementation of their rule base onto their firewall devices.

They implemented AlgoSec Firewall Analyzer and AlgoSec FireFlow, as well as AlgoBot, AlgoSec's ChatOps solution.

“AlgoSec has saved us a lot of time in managing our rule base.”

IT Team Specialist

continued

THE SOLUTION

AlgoSec Firewall Analyzer ensures security and compliance by providing visibility and analysis into complex network security policies.

AlgoSec FireFlow improves security and saves security staffs' time by automating the entire security policy change process, eliminating manual errors, and reducing risk.

AlgoBot is an intelligent chatbot that handles network security policy management tasks. AlgoBot answers business user's questions, submitted in plain English, and automatically assists with security policy change management processes – without requiring manual inputs or additional research.

THE RESULTS

Some of the ways the company benefitted from using AlgoSec include:

Visibility and topology mapping – They are able to get a picture of their entire network and view traffic flows to each network device.

Optimized firewall rules – They are able to adjust the placement of their rules, placing their most used rules higher in the rule base, improving performance, and also checking for unused objects or rules to clean up, removing unused rules, improving firewall performance.

Improved communication and transparency for time-based rules – Before time-based rules expire (rule with an expiration date), the requester is automatically notified and asked if the rule should be extended or removed.

Better, more refined rule requests – By first gathering information from AlgoBot, rule requests are better focused. Internal customers are able to check if rules are already in place before making requests, therefore avoiding requests that are already covered by existing rules.

Empower internal stakeholders – Able to save the IT team's time by empowering internal stakeholders to use AlgoBot to get the answers themselves to traffic queries.

Met change implementation SLAs – By implementing their rules with AlgoSec, the company meets their internal SLAs for change implementation.

Streamlined auditing processes – By documenting the changes they made in the firewalls, who made them, and when, their audit processes are streamlined.

Zero-touch automation – Automatically implementing rules in multiple firewalls simultaneously ensures policy consistency across multiple devices, while preserving staff resources. This also eliminates the need to use the management consoles from individual vendors, saving time and reducing misconfigurations.

Staff efficiencies – Hundreds of monthly change requests are able to be managed by a single staff member. He would not be able to do it without AlgoSec.

The company switched from a competing solution because AlgoSec's was more user-friendly and provided greater visibility than the solution they were previously using. They are also impressed with AlgoSec's scalability. "The initial setup is really easy. It has been running flawlessly since installation. Even upgrades are pretty straightforward and have never given us problems," they noted.