BUSINESS-DRIVEN SECURITY MANAGEMENT FOR LOCAL GOVERNMENTS

Local government agencies are complex, running multiple network devices both inside and outside of the data center, in public and private clouds, and using a myriad of networking and security tools. They struggle with legacy technology that require extensive maintenance, have limited budgets, and maintain highly sensitive and confidential data that are constantly under attack.

Local government agencies' network and security operations teams are slowed down by manual, slow, and error-prone security change management processes, and the significant effort required to maintain complex network security environments and meet ever changing compliance requirements. It often takes several days, or even weeks, to process a single change across a complex enterprise environment.

Key security policy management challenges for local governments include:

- Complying with regulations and maintaining compliance
- Implementing security policy changes rapidly
- Visualizing traffic flows across hybrid networks
- Assessing which changes introduce new risks
- Connecting vulnerabilities to business processes
- Identifying unused, obsolete, or duplicate security rules

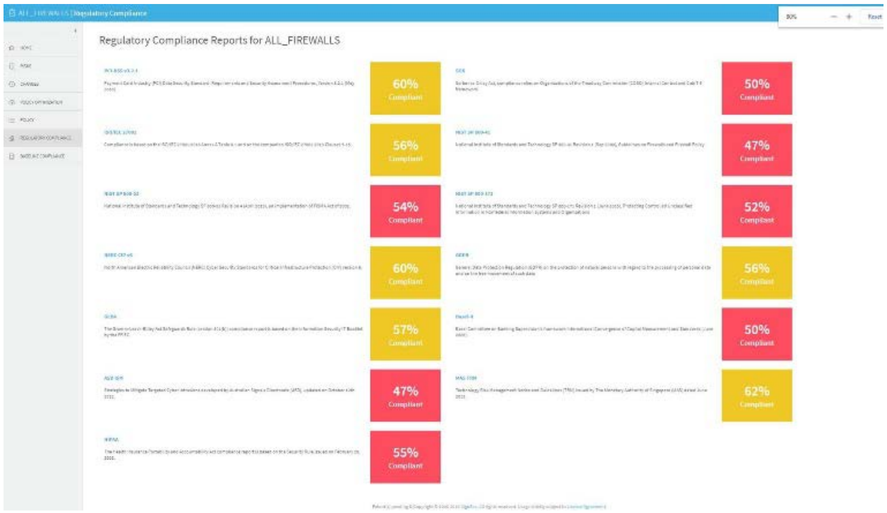
Key Benefits

- Get consistent security management across any heterogeneous network environment.
- Deploy applications faster by automating network security change management processes.
- Avoid security device misconfigurations that cause outages.
- Migrate application connectivity to the cloud quickly and easily.
- Reduce the costs and efforts of firewall auditing.
- Facilitate effective communication between security teams and application owners.
- Tie security incidents directly to business processes.

Automate Firewall Auditing and Ensure Continuous Compliance

Agencies need to comply with many different regulations, and a plethora of policies and rules governing cybersecurity standards and personal or financial data. Maintaining continuous visibility over so many rules and regulations is difficult.

AlgoSec automatically generates pre-populated, audit-ready compliance reports for leading industry regulations, including SOX, BASEL II, GLBA, PCI DSS, ISO 27001, FISMA, and internal policies — which helps reduce audit preparation efforts and costs. AlgoSec also uncovers gaps in the compliance posture and proactively checks every change for compliance violations.



Automate Security Policy Change Management

Change management processes are slow. Processing a single change in a complex environment, which often has hundreds or more monthly changes, can take days, or even weeks.

With AlgoSec's automated security policy management, you can process security policy changes in minutes, avoiding guesswork, and manual errors, while reducing risk and enforcing compliance. Using intelligent, highly customizable workflows, AlgoSec automates the entire security policy change process — from planning and design through submission, proactive risk analysis, implementation, validation, and auditing — all with zero-touch.

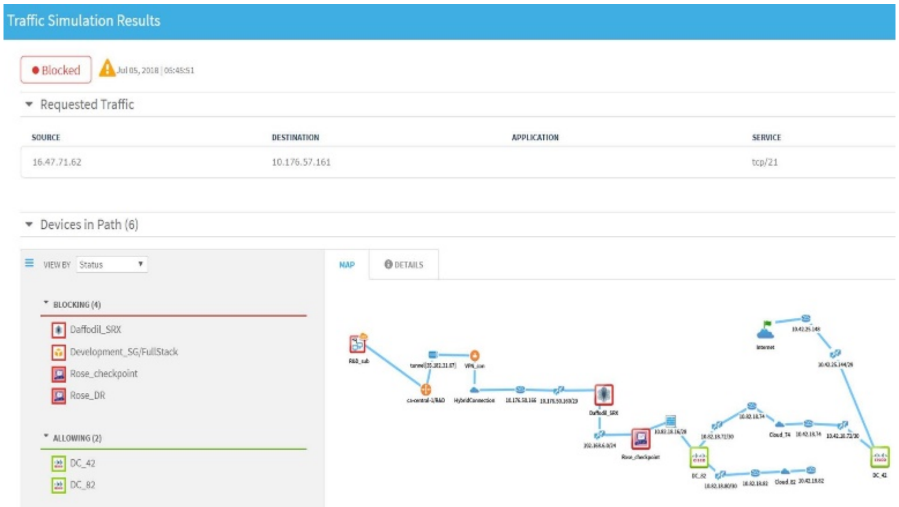
As part of this process, AlgoSec automatically analyzes all change requests and identifies all devices across the network which will be impacted by the request, identifies risks, and then specifies the most optimal and secure implementation for change requests that utilize existing firewall rules and objects whenever possible, reducing policy clutter and complexity. Unnecessary change requests are closed, and requestors are notified — helping to prevent up to 30% of change requests from being unnecessarily processed.

Gain Visibility into the Entire Security Network

Organizations are running a disarray of networks – from on-premise legacy systems that need constant maintenance, to the latest and greatest, such as public/private clouds and SDNs – and no idea how traffic flows between them. Network traffic resides in its own silo, and agencies have created data islands. Without visibility into traffic flows, organizations risk data leakage.

AlgoSec simplifies daily network operations by automatically generating an interactive topology map. This map scales to the largest and most complex networks, seamlessly supporting firewalls, SDNs, routers, load balancers, and web proxies, as well as network subnets and security zones.

Using the map, security and operations teams gain instant visibility into the impact of security policies on network traffic, and can quickly troubleshoot connectivity issues, plan changes, and perform "what-if" traffic queries.



Traffic Simulation Results

● Blocked Jul 05, 2018 | 05:45:51

Requested Traffic

SOURCE	DESTINATION	APPLICATION	SERVICE
16.47.71.62	10.176.57.161		tcp/21

Devices in Path (6)

VIEW BY Status

BLOCKING (4)
- Daffodil_SRX
- Development_SG/FullStack
- Rose_checkpoint
- Rose_DR

ALLOWING (2)
- DC_42
- DC_82

Proactively Assess and Manage Risk

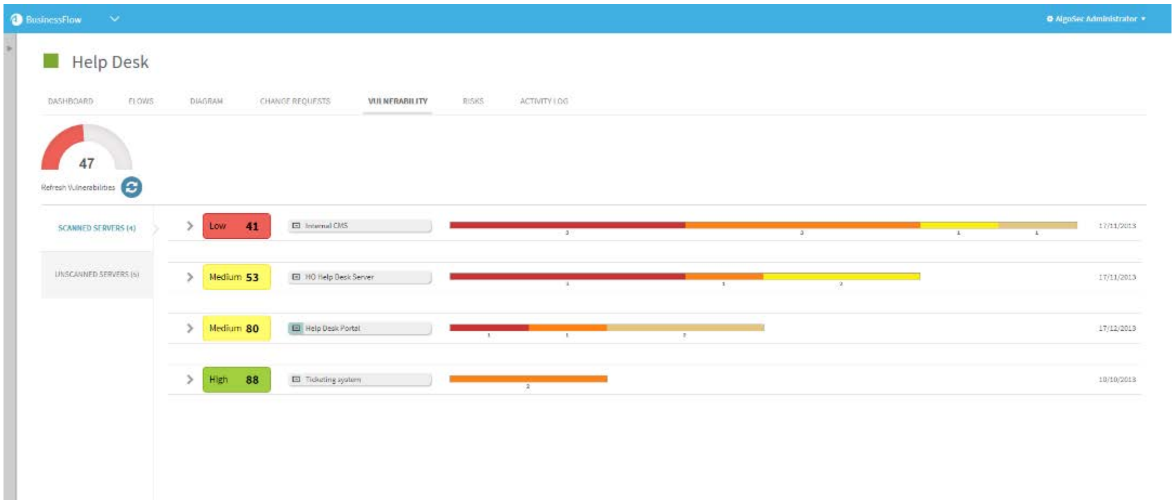
It is difficult to make new changes because government agencies are notoriously risk-averse and under resourced. Thus, new initiatives are often avoided due to the fear of introducing new risk.

AlgoSec proactively assesses the impact of every proposed change to the security policy before it is implemented -- minimizing risk, avoiding outages, and ensuring compliance. AlgoSec leverages the broadest risk knowledgebase which includes industry regulations, best practices, and organization-defined policies. As application components, connectivity requirements and vulnerabilities change, AlgoSec ensures agencies have up-to-date and accurate information to prioritize risk.

Link Vulnerability to Business Processes

High walls and siloed operations make navigation difficult. It's not clear who owns risk and thus who is responsible for fixing it. As a result, technical risk accumulates and there is a lack of accountability between application owners and technical teams.

Through its integration with leading vulnerability scanners, AlgoSec links vulnerabilities to their business processes, giving you the information that you need to prioritize, and mitigate risks. This includes applications, servers, network, security devices and traffic flows.



Help Desk

47

SCANNED SERVERS (4)

UNSCANNED SERVERS (5)

Low 41	Internal CMS	17/11/2013
Medium 53	HO Help Desk Server	17/11/2013
Medium 80	Help Desk Portal	17/12/2013
High 88	Ticketing system	10/10/2013

Cleanup, Recertify, and Optimize Security Policies

Legacy systems are a significant part of many IT systems, yet they pose efficiency and security issues. Substantial IT spending is devoted to maintaining aging legacy systems, which pose efficiency, cybersecurity, and mission risk issues. Over the years, your firewalls have accumulated thousands of rules and objects, and many of these rules are now obsolete. Bloated rulesets not only add complexity to daily tasks but also impact the performance of your firewalls, resulting in decreased hardware lifespan and increased Total Cost of Ownership.

AlgoSec continuously analyzes existing network security policies and provides actionable recommendations to help cleanup and reduce risk. AlgoSec can uncover unused, obsolete, or duplicate rules, initiate a recertification process for expired rules, provide recommendations on how to consolidate or reorder rules for better performance, and tightens overly permissive “ANY” rules — without impacting business requirements. All changes are defined, implemented, and validated through AlgoSec’s automated change management process.