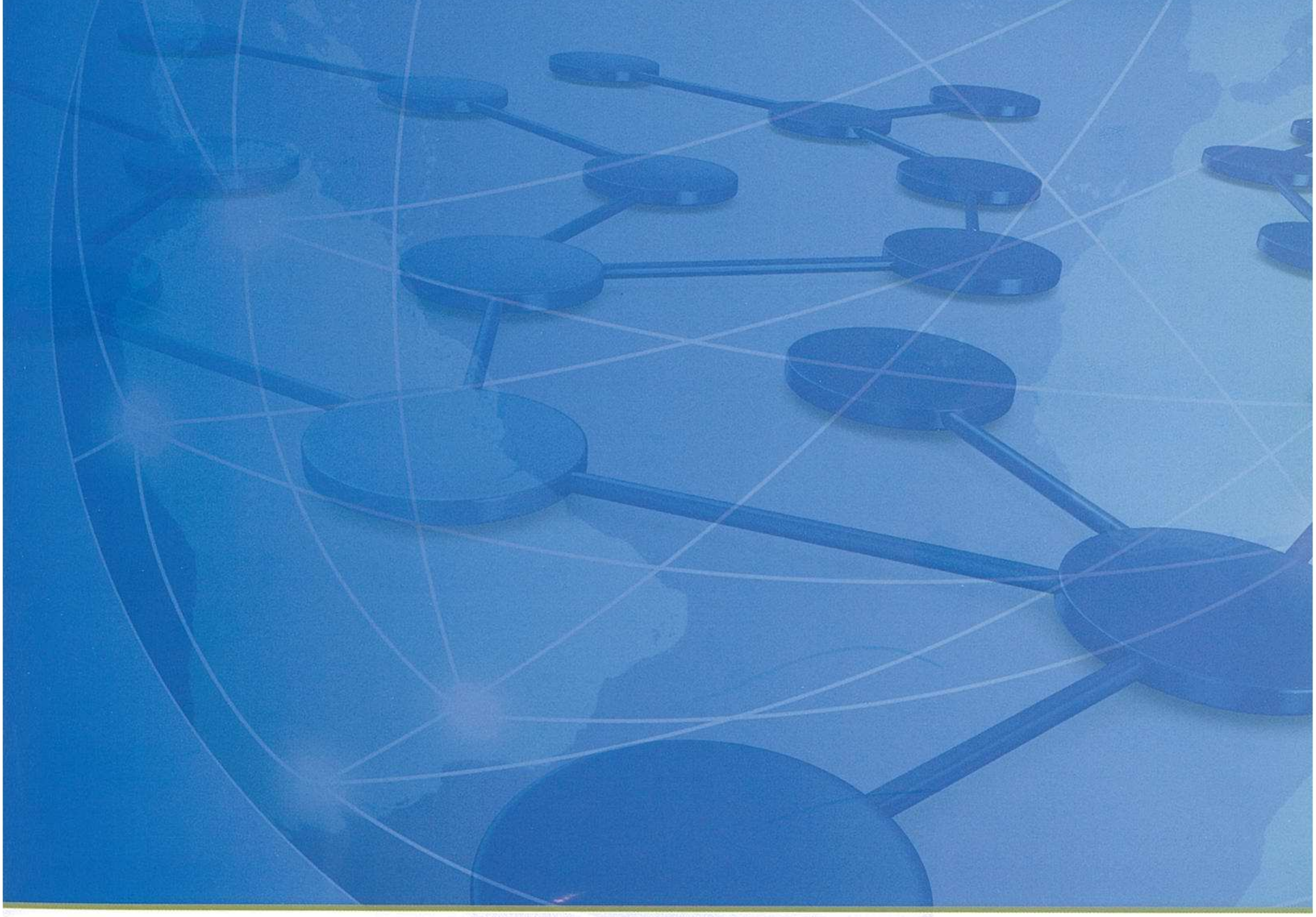
AlgoSec Security Management Suite

Intelligently Automating Firewall Policy Management



algosec

Security Management, Made Smarter.

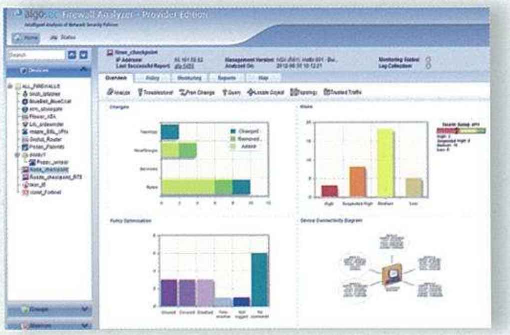
AlgoSec.com

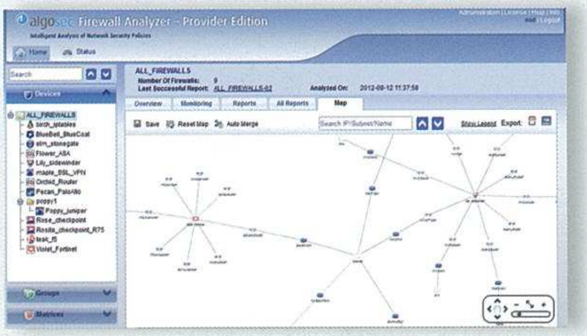
AlgoSec Firewall Analyzer

Intelligent Analysis of Network Security Policies

AlgoSec Firewall Analyzer (AFA) automates the management of complex security policies to ensure network security devices are properly configured. AFA enables security and operations teams to:

- Reduce firewall audit preparation time by 80%
- Streamline firewall operations and improve firewall performance
- Ensure a tighter security policy for improved protection against cyber-attacks





Gain Visibility of Your Security Policy

AFA provides visibility of complex networks and security policies to make daily firewall operations easier and more effective. AFA automatically generates an interactive topology map of all network firewalls and routers, subnets and zones, and delivers instant visibility of the impact of security policies on network traffic through powerful troubleshooting, change planning and "what-if" queries.

Monitor All Network Security Policy Changes

All changes in the network security policy are monitored and logged and administrators receive real-time e-mail alerts for unauthorized or risky changes.

Clean up and Optimize Firewall Rulesets

AFA discovers unused, covered, duplicate and expired rules and objects, and can even consolidate similar rules. Additionally, AFA provides explicit recommendations on how to reorder rules for optimal firewall performance while retaining the policy logic.

Ensure a Tighter Policy without Impacting Operations

AlgoSec Intelligent Policy Tuner™ reduces risk without impacting business needs by automatically identifying and tightening overly permissive rules (e.g. ANY Service, Application, etc.) based on actual usage patterns.

Discover and Mitigate Risky Firewall Rules

All risks and their associated rules in the firewall policy are identified and prioritized. AFA relies upon the broadest risk knowledgebase, consisting of industry regulations and best practices, as well as customized corporate policies, to ensure more risks are uncovered.

Mitigate Cyber Threats with Baseline Configuration Compliance

Define baselines for device configurations to minimize system risks that can be exploited by cyber criminals and generate reports to identify non-compliant configurations.

Generate Automated Audit and Compliance Reports

AFA automatically generates reports for corporate and regulatory standards, such as PCI-DSS, SOX, FISMA and ISO, to greatly reduce audit preparation efforts and costs - by as much as 80%. AFA can aggregate findings across multiple firewalls through a single report, which provides more holistic visibility into risk and compliance associated with a group of devices.

Simplify Firewall Migrations

AFA facilitates firewall migration and upgrade projects by comparing the policies of different firewalls and vendors. Additionally, powerful queries enable operations teams to locate IP addresses and ensure that all connections are in place.

> **"Now we can get in a click of a button what took two to three weeks per firewall to produce manually."**
>
> **Marc Silver,** Security Manager

Discovery

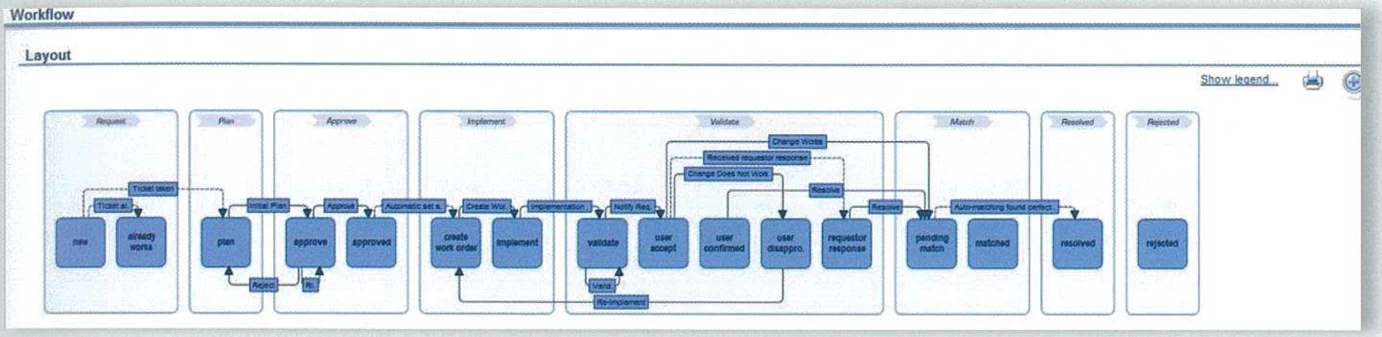
AlgoSec FireFlow

Security Policy Change Automation

AlgoSec FireFlow automates the entire security policy change workflow – from submission and design to risk analysis, implementation, validation and audit - enabling security and operations teams to:

- Reduce the time required to process firewall changes by as much as 60%
- Increase accuracy and accountability of change requests
- Enforce compliance and mitigate risk from improper and out-of-process changes

FireFlow seamlessly integrates with existing service desk ticketing systems to add firewall-aware intelligence and can easily be customized to match each organization's specific business processes.



Automate the Security Policy Change Workflow

FireFlow delivers out-of-the-box workflows for adding new rules, removing rules, changing objects and recertifying rules, enabling organizations to tackle more real-life scenarios and improve operational efficiency.

Analyze Change Requests to Ensure Compliance and Mitigate Risk

FireFlow automatically analyzes every proposed change - before they are implemented – to ensure compliance with regulatory and corporate standards. FireFlow leverages the broadest risk knowledgebase that includes industry best practices, regulations such as PCI-DSS and SOX, as well as corporate-defined policies.

Eliminate Guesswork with Intelligent Change Management Design

FireFlow's topology-aware algorithms automatically verify change requests against network traffic to detect unneeded ("already works") changes and notify requestors, which can reduce up to 30% of change requests from being unnecessarily processed. FireFlow's detailed and actionable recommendations specify the most optimal and secure implementation, pinpointing the relevant devices and rules to add, delete or edit.

Save Time and Avoid Manual Errors with Automatic Policy Push

FireFlow can automatically implement recommended policy changes on Check Point firewalls and generate Cisco CLI commands.

Prevent Mistakes and Unauthorized Changes through Auto-Validation and Reconciliation

FireFlow automatically validates the correct execution of change requests to prevent the pre-mature closing of tickets. Auto-matching prevents unauthorized changes by detecting actual policy changes and correlating them with request tickets.

Customize Change Workflows to Meet Your Unique Requirements

FireFlow makes it easy to tailor workflows to each organization's specific requirements and its flexible roles and workflow logic ensure accountability and governance. Additionally, pre-populated templates save time and improve communication and clarity between requestors and firewall administrators.

Track and Audit the Entire Change Lifecycle

Detailed reports track the entire change lifecycle, providing SLA metrics and greatly simplifying auditing and compliance efforts.

Integrate with Existing Change Management Systems (CMS)

FireFlow seamlessly integrates with existing CMS, such as BMC Remedy, HP Service Manager and CA Service Desk Manager. Status of tickets created in the CMS is continuously updated.

> **"With AlgoSec, it now takes us half the time to employ firewall changes.** Plus the solution provides us with intelligence that reduces human error and risk."
> **Saúl Padrón,** Manager of Information Security

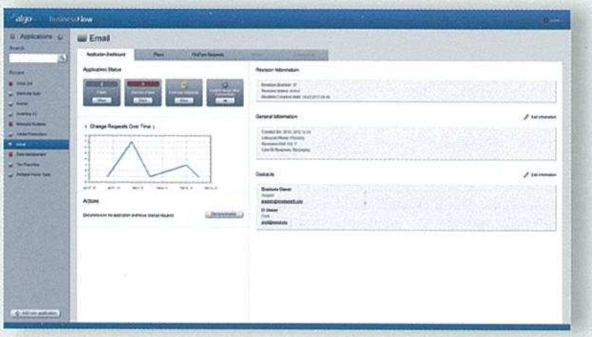
Telefonica

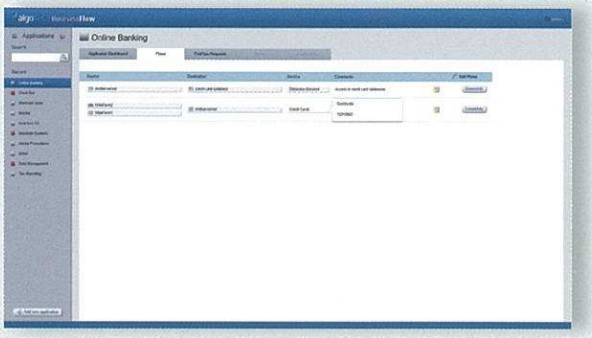
AlgoSec BusinessFlow

Application-Centric Security Policy Management

AlgoSec BusinessFlow delivers innovative, application-centric security policy management that boosts business agility and the availability of enterprise applications. BusinessFlow allows application connectivity requests to be made in application terms and provides visibility of the impact of network changes on application availability, enabling application owners and network security teams to:

- Ensure faster service delivery and improved application availability
- Improve visibility of business applications connectivity requirements
- Deliver tighter security processes and policy





Automatically Translate Connectivity Requirements to Firewall Rules

BusinessFlow enables changes for evolving application connectivity requirements to be quickly and accurately processed by automatically computing the necessary changes to the underlying firewall rules and triggering the relevant change requests in AlgoSec FireFlow.

Assess the Impact of Network Changes on Application Availability

BusinessFlow helps key stakeholders understand the impact that network changes, such as server migrations, may have on business applications and trigger the necessary firewall change requests to ensure application availability.

Ensure Secure Decommission of Applications

Safely remove network access that is no longer required for decommissioned applications to ensure that the security policy is hardened without impacting the availability or performance of other business applications.

Enhance Visibility through a Central Application Connectivity Portal

A consolidated and up-to-date view of required application connectivity enables security and network teams to communicate more effectively with business application owners for accelerated service delivery.

Discover and Map Underlying Rules and ACLs to Applications

Powerful discovery capabilities enable firewall and router access rules to be mapped to existing applications, dramatically reducing the time and effort to populate the application repository.

Deliver a Complete Audit Trail of All Changes

Audits and proof of compliance are simplified by maintaining a complete history of every change made to the application supporting both internal and external compliance mandates.

Tight Integration with the AlgoSec Suite

BusinessFlow leverages AlgoSec Firewall Analyzer for policy analysis, traffic simulation and visualization, and AlgoSec FireFlow for security policy change management.

Integration with Existing CMDB Systems

BusinessFlow leverages information in existing CMDB systems to simplify implementation and management.

> **"Organizational networks and the applications using them are more complex than ever. Having a more clear view of a network change on the application or service translates to a simpler security policy and fewer blocks of legitimate activity."**
>
> **Greg Young,** Research Vice President, Gartner

Gartner

Specifications

Devices Supported

Check Point	FireWall-1®, Provider-1®, SmartCenter	v3.0 and up ,NG, NGX, Software Blade Architecture (R7x) – including Application Control and Identity Awareness
	VSX	All versions
	Security Gateway VE	All versions
Cisco	PIX, ASA Series	v4.4 and up
	Firewall Services Module (FWSM)	v1.0 and up
	Cisco Router Access Control Lists	All versions
	Cisco Layer-3 Switches	All versions
	Nexus Routers	All versions
	Cisco Security Manager	v4.3
Juniper	NetScreen Series	v5.0 and up
	Network and Security Manager (NSM)	v2008.1 and up
	SRX Series	All versions
Fortinet	Fortigate	FortOS 3.x and up, including VDOM
	FortiManager	v4.x
Palo Alto Networks	PAN-OS	v4.x and up
McAfee	Firewall Enterprise (formerly Sidewinder)	v7.x and up
Blue Coat Systems	Proxy SG	v5.x and up

Supported Devices for Change Monitoring*

F5	Big-IP Family
Juniper	Secure Access SSL VPN
Linux	Netfilter/Iptables
Stonesoft	StoneGate
WatchGuard	XTM

*Additional devices can be added via the AlgoSec Extension Framework

Supported Change Management Systems**

BMC	Remedy
HP	Service Manager
CA	Service Desk Manager

**Additional change management systems can be supported by AlgoSec professional services

Evaluate Today. Request a free 30-day evaluation at: AlgoSec.com/Eval

algosec

Security Management, Made Smarter.

Follow Us On:

Global Headquarters
265 Franklin Street
Boston, MA 02110
USA
+1-888-358-3696

EMEA Headquarters
33 Throgmorton Street
London, EC2N 2BR
United Kingdom
+44 207-099-7545

APAC Headquarters
10 Anson Road, #14-06
International Plaza
Singapore 079903
+65-3158-2120