

A photograph of a man in a white shirt smiling while working on a laptop. The image is partially obscured by a large blue graphic element that resembles a stylized 'A' or a network node. To the right, there is a circular inset showing a network diagram with nodes and connecting lines.

# AlgoSec Security Management Suite

## Intelligently Automating Firewall Policy Management

### Managing Security in Complex Network Environments

In the battle to safeguard the organization's network, the security policy continues to grow in size and complexity, with hundreds or thousands of rules and objects to manage across multiple vendor devices and geographies. Manual processes traditionally used for performing risk analysis, auditing and compliance and change management are not only labor-intensive but also error-prone. Today's organizations must manage security policies in a new way that enables them to increase operational efficiency and reduce risk.

### The Market Leading Solution for Network Security Policy Management

More than 800 enterprises, Managed Service Security Providers (MSSPs), consultants and auditors in over 40 countries use AlgoSec's Security Management Suite, the market leading solution for network security policy management. Comprised of AlgoSec's Firewall Analyzer (AFA) policy analysis solution and the AlgoSec FireFlow change automation solution, the Security Management Suite enables security and operations teams to effectively manage complex security policies of multi-vendor firewalls, VPNs, routers and related devices. The AlgoSec Security Management Suite simplifies auditing and compliance, streamlines operations and increases accuracy and governance.

### Better Analysis and Superior Automation Deliver the Best ROI

Powering the Security Management Suite, AlgoSec's patented Deep Policy Inspection™ technology delivers superior policy analysis, uncovering more results with greater accuracy. By automating more processes, Deep Policy Inspection enables organizations to improve operational efficiencies by 60 percent or more, while strengthening their security posture.

# AlgoSec Firewall Analyzer

## Intelligent Analysis of Network Security Policies

AlgoSec Firewall Analyzer (AFA) enables network operations and security teams to effectively audit and analyze complex network security policies. Providing visibility across multi-vendor environments, AFA allows organizations to easily track policy changes, clean up and optimize rulesets, plan changes and identify risky and non-compliant rules. AFA's unique combination of intelligent automation with complete network visibility ensures devices are properly configured at all times. Using AlgoSec's Deep Policy Inspection technology, AFA uncovers more risks with greater accuracy, improving security and compliance while increasing operational efficiency.

### Risk Analysis and Mitigation

All risks and their associated rules in the firewall policy are identified and prioritized. Broadest risk knowledgebase, consisting of industry regulations and best practices, as well as customized corporate policies, ensures more risks are uncovered.

### Automated Compliance Reports

Automatically generated reports for corporate and regulatory standards, such as PCI-DSS, Sarbanes-Oxley and ISO 27001, greatly reduce audit preparation efforts and costs.

### Topology-Aware Policy Visibility

Powerful troubleshooting, change planning and "what-if" queries provide instant visibility into the effects of security policies on network traffic.

### Change Monitoring and Alerting

All changes in the network security policy are monitored and logged. Administrators can opt to receive e-mail alerts for unauthorized or risky changes.

### Policy Cleanup and Optimization

Detailed reports flag unused, shadowed, duplicate and expired rules and objects, and can even consolidate similar rules.

### Intelligent Rule Reordering

Explicit recommendation on how to reorder rules for optimal firewall performance while retaining the policy logic.

### Intelligent Policy Tuner™

Overly permissive rules (e.g. ANY Service) are tightened based on actual usage patterns, without impacting business needs.

### Group Reports

A single report provides visibility into risk and compliance associated with a group of devices.

### Firewall Migration

Policies of different firewalls and vendors are easily compared to facilitate upgrade and migration projects.

### Multi-Domain Support

Support for multiple domains, complete with segregation of duties, enables managed service providers to centrally service multiple customers.

### Extensible Architecture

The AlgoSec Extension Framework (AEF) monitors changes across a wide array of devices, including application accelerators, web proxies and load balancers.

## Highlights

- Generate automated audit and compliance reports
- Discover and mitigate risks in the firewall policy
- Cleanup and optimize firewall rulesets
- Monitor all network security policy changes
- Effectively troubleshoot network problems

"AlgoSec Firewall Analyzer is saving us valuable time by replacing the manual and labor intensive process of firewall operations management with an intelligent and automated solution"

**Anton Spitzer**  
Infrastructure Services,  
Porsche Informatik



The AlgoSec Security Management Suite is the only product suite of its kind to receive a 5/5 rating from SC Magazine.

# AlgoSec FireFlow

## Intelligent Automation of Network Security Changes

AlgoSec FireFlow intelligently automates the workflow of network security policy changes. FireFlow replaces manual and error-prone processes with proactive network and risk-aware automation, dramatically reducing the time required to process changes, ensuring compliance and increasing accuracy. FireFlow is fully customizable and integrates with existing change management systems, increasing operational efficiency while tailoring to existing business processes.

### Customizable Workflow Automation

A visual workflow editor makes it easy to define each organization's business processes. Flexible roles and workflow logic ensure accountability and governance. Out-of-the-box workflows are provided for adding rules, removing rules and changing objects.

### Preliminary Change Planning

New requests are automatically verified against network traffic to prevent unneeded changes and pinpoint the exact devices which need to be changed.

### Customizable Request Templates

Pre-populated templates save time and improve communication and clarity between requestors and firewall administrators.

### Proactive Risk and Compliance Analysis

Before implemented, every change is analyzed to ensure compliance with regulatory and corporate standards. Broadest risk knowledgebase includes industry best practices, regulations such as PCI-DSS and SOX, as well as customized corporate policies.

### Design and Implementation Planning

Detailed recommendations specify the most optimal and secure implementation, including all relevant devices and rules to add, delete or edit.

### Automatic Policy Push (Optional)

Unique ActiveChange™ technology automatically implements recommended policy changes, saving time and avoiding manual errors.

### Auto-Validation and Matching

Correct execution of requests is validated to prevent re-opening of tickets. All detected changes are matched to requests and mismatches reported.

### Audit-Ready Reports

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

### Integration with Change Management Systems

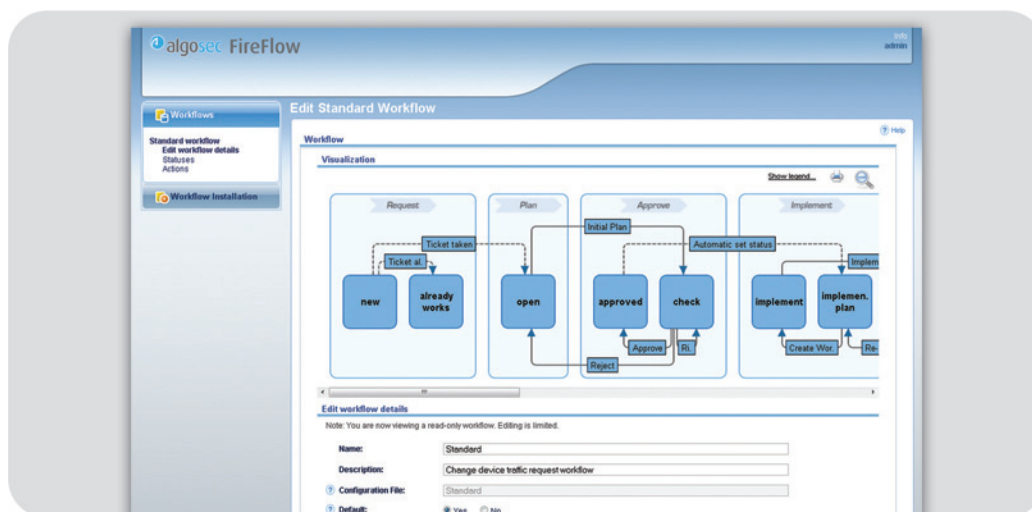
Seamless integration with existing Change Management Systems (CMS), such as BMC Remedy and HP ServiceCenter. Status of tickets created in the CMS is continuously updated.

### Highlights

- Process network security changes in less than half the time
- Avoid unneeded changes
- Proactively assess the risk of every proposed change
- Ensure changes comply with regulatory and corporate standards
- Easily track and audit the entire change lifecycle
- Improve accuracy, visibility and governance

"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



# Specifications

## Supported Devices

Check Point	FireWall-1®, Provider-1®, SmartCenter	v3.0 and up
	VSX	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
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

OPSEC



CERTIFIED



JUNIPER  
NETWORKS



## Supported Devices for Change Monitoring\*

BlueCoat	Proxy Server and WebFilter
F5	Big-IP Family
Juniper	Secure Access SSL VPN
Linux	Netfilter/Iptables
McAfee	Sidewinder
Stonesoft	StoneGate
Palo Alto Networks	PA Series

\*Additional devices can be added via the AlgoSec Extension Framework

## System Requirements

The AlgoSec Security Management Suite can be delivered as software only, or preloaded on a hardened virtual or physical appliance.

Physical appliances can be deployed in high-availability mode and support load-sharing for increased scalability.

Software	Memory	2GB
	CPU	3Ghz
	Storage	300 GB (2GB and additional 50MB per report)
	Operating System	Red Hat Enterprise Linux v4/v5 CentOS 4 - 5 Microsoft Windows 2000/XP/Vista (VMWare)
	Browser	Internet Explorer 7.0 or higher Firefox 3.6 or higher
Virtual Appliance	VMware virtual appliance can run on a hosting Windows server with 1GB of RAM (2GB RAM or more is recommended).	
AlgoSec Appliance	AlgoSec 1020 – low cost entry level, best for up to 150 firewalls AlgoSec 1080 – High-performance, best for up to 1000 firewalls AlgoSec 1160 – Enterprise level, best for up to 2000 firewalls	

**AVANTEC**  
Competence. Security. Trust.

AVANTEC AG • www.avantec.ch  
CH-8003 Zürich • CH-3011 Bern