AlgoSec Firewall Analyzer

Product Datasheet

The AlgoSec[TM] Firewall Analyzer (AFA) is a firewall operations and security risk management solution that provides automated, non-intrusive firewall, router and VPN audit and analysis. It helps network administrators improve their ability to assess their router and firewall configurations, track changes and improve performance. With its exclusive topology-aware technology AFA intelligently automates the analysis of routing tables, security zones, rules and logs to deliver cost-savings and improved governance.

Supported Devices

AFA *fully supports* the following devices:
- **Check Point® FireWall-1®** and **Provider-1®**
  Versions: 3.0, 4.0, 4.1, NG, NGX
  Platforms: Solaris, SecurePlatform[TM], Nokia IPSO, VSX, Crossbeam, Nortel, Linux, UTM-1, and Windows English language locale (US or UK)
- **Cisco PIX, ASA** and **FWSM**
  Versions: PIX/ASA v4.4 and up, FWSM v1.0 and up
- **Cisco Router Access Control Lists**
  Versions: All
- **Cisco Layer-3 Switches**
  Versions: All
- **Juniper Netscreen**
  Versions: 5.0 and up

AFA offers support as listed for the following devices:
- **Fortinet Fortigate**
  Versions: All
  Features: Policy change monitoring; Policy rules view; Full routing table analysis, including a detailed firewall connectivity diagram and traffic query capabilities; Full support for Fortigate Virtual Domains (VDOMs); Supported in AlgoSec FireFlow

AFA supports the following devices for policy change monitoring (E-mail alerts and Web changes view):
- **Juniper JunOS**-based routers and firewalls
- **Juniper Secure Access** (SSL VPN)
- **Blue Coat Proxy Server** and **Web Filter**
- **McAfee Firewall Enterprise (SideWinder)**
- **Palo Alto Networks**
- **Linux netfilter iptables**
- **StoneSoft StoneGate**
- Additional devices added via the AlgoSec Extension Framework (AEF)

System Requirements

The following Linux distributions are supported:
- Red Hat Enterprise Linux 4, 5
- CentOS 4, 5
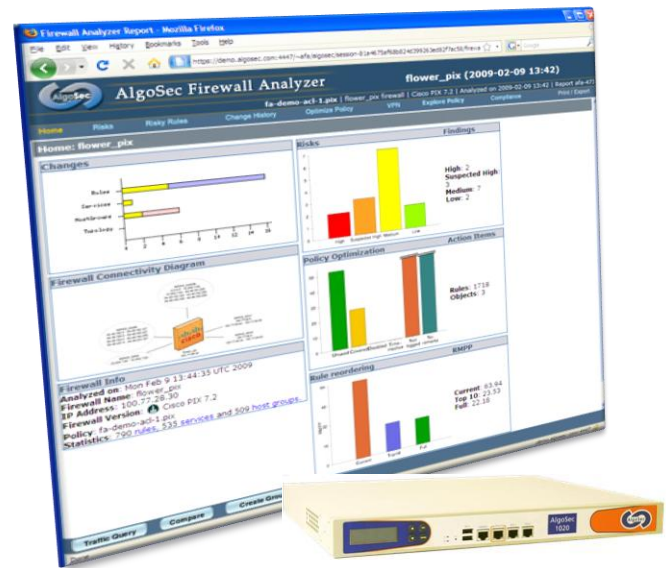
AFA runs on the following hardware:
- A server with 32-bit x86 processors or compatible. Recommended server specifications:
  - > Memory: 2GB RAM
  - > CPU: 3GHz
  - > Storage: 300GB
    (2GB and additional 50MB per report)
- AlgoSec 1000 Series Appliance

Software Appliance

AFA is available as a VMware appliance, using a VMware Player/Server over hosting Microsoft Windows 2000/XP/Vista, Linux or VMware ESX Server.

AlgoSec 1000 Series Appliance

AFA is available on two hardware appliance models, providing customers fast implementation solution in-a-box:
- **AlgoSec 1020** – low cost entry level, best for up to 100 firewall environment
- **AlgoSec 1080** – high-performance enterprise level, best for up-to 750 firewall environment

The appliances are hardened and provided with supplementary system management tools.

Regulations and Standards Compliance

Automatically produced compliance reports help to ensure your firewall policies are configured according to various compliance and regulatory standards, while saving your auditors and operations team significant time and effort:

- Payment Card Industry Data Security Standard (PCI-DSS)
- ISO/IEC 27001
- Sarbanes Oxley Act (SOX)
- BASEL-II
- Financial Instruments and Exchange Law (J-SOX)

AlgoSec Firewall Analyzer Features and Benefits

AlgoSec Firewall Analyzer Operations & Optimization

Features	Benefits
Firewall analysis and reports	Visual display of the firewall policy, topology, traffic, rules and objects. It also includes analysis of the routing table and provides a connectivity diagram. Shows changes from previous reports on the same firewall.
Group Report	Create a report on a group of firewalls with either predefined or ad-hoc firewall definitions.
Customized report scheduling	Schedule an analysis on a per-firewall or group of firewalls based on pre-defined intervals (daily, weekly, monthly, upon policy install, etc) and issue a report.
Offline Web interface	Offer offline policy store to deliver unprecedented visibility and insight to ensure current configurations match mandated policies.
Report comparisons	Compare any two reports – either the same firewall or different firewalls or different firewall vendors. Show the changes in traffic, rules, services, host groups, topology and objects.
Real time monitoring	Continuously poll firewall policy changes, update monitoring web page and send email alerts when a change is detected.
email notifications	Send emails to pre-assigned users following a firewall analysis with the summary of the analysis and changes.
Change Planning Query	Query a single firewall or a group of firewalls (even of different vendors) to optimally plan rule changes based on actual routing table and topology.
Troubleshooting Query	Query a single firewall or a group of firewalls (even of several different vendors to troubleshoot a connectivity problem, based on actual routing table and topology.
Basic compliance	Track every rule, object and routing change – to achieve basic compliance.
What-if analysis	Analyze a firewall policy before actually pushing it into production. Allows planned changes to be tested to ensure that the change in policy will produce the required results.
Rule optimization and cleanup	Identify unused, covered, redundant special case, disabled, time in-active and unused NAT rules which are candidates for removal. List rules that may not conform to company policies, including rules without comments, without logs and rules with non-compliant comments.
Object cleanup and audit	List unattached, empty, duplicate and unused objects which are candidates for removal.
Usage analysis	Show unused rules, unused objects within rules, the most and least used, and last date of use.
Intelligent rule re-ordering	Explicit recommendation of new positions to the rules in order to improve the firewall performance while retaining the policy logic.
VPN cleanup and audit	Show VPN parameters including unused users, unattached users, expired users, users about to expire, unused groups, unattached groups and expired groups.
VPN analysis	Present the VPN parameters also in the change history page and in email notifications.

AlgoSec Firewall Analyzer Risk & Compliance Module

Features	Benefits
Deep risk analysis	Identifies every packet the firewall may encounter. Automatically maps topology and identifies the most serious threats based on industry best practices, prioritizes subsequent risks and offers guidance on what and how to remediate.
Automatically populated compliance reports	Generates automatically populated compliance reports to assure continued adherence to external regulatory standards including PCI-DSS, SOX, ISO, BASEL-II and J-SOX, providing turnkey reports to the end-user/auditor.
Matrix (multi-tiered) risk analysis	Analyzes several firewalls together, taking into account their relative hierarchy in the network. Trigger is allowed between risky zone to a secured zone by ALL firewalls in the multi-tierd structure.
Group Compliance reports	Run a single compliance report that includes a group of a large number of firewall to view overall corporate compliance on a single report.
Continuous security audit	Provide complete audit trail and replace error prone manual task to ensure alignment with security policy.
Identify risky rules	Identify all rules that allow risky traffic and should be reviewed. Analysis is based on routing table examination and industry best practices.
Customize risk assessment	Customize out-of-the-box risks creating customer specific risk profiles, user-defined zone-types and trusted traffic. This allow customer to easily implement their corporate security policy.
"Changes in risks" alert	Send emails to pre-assigned users following a change to the security posture relative to previous analysis.
VPN Risk analysis	Add risks associated to VPN rules and VPN objects to the Change History page and to email notifications.

North America Headquarters
1900 Campus Commons
Drive Suite 100
Reston VA 20191
888-852-7482

EMEA Headquarters
145-157 St. John Street
2nd Floor
London EC1V 4PY
44-0-208-099-7504

Research & Development
32 Shaham Street
Petah Tikva, Israel

http://www.algosec.com

Security. Visibility. Governance.