OGREN group

SECURITY REPORT

Firewall Analysis Saves Time Keeping Application Paths Clear

Firewall Analysis vendors are at a crossroads in planning to broaden their focus to sustain revenue growth. The core competency of Firewall Analysis, an on-demand study of complex sets of firewall rules to ensure new rules keep application paths clear, is generating enough customer traction to encourage vendors to pursue higher growth markets. The $131 million 2013 Firewall Analysis market participants are evolving to application security, threat assessment, or enterprise security management solutions.

The Ogren Group estimates the market for Firewall Analysis products and services will be $131 million in 2013, and predicts growth at a compound annual growth rate of 19% to $313 million by 2018, as shown in Exhibit 1.

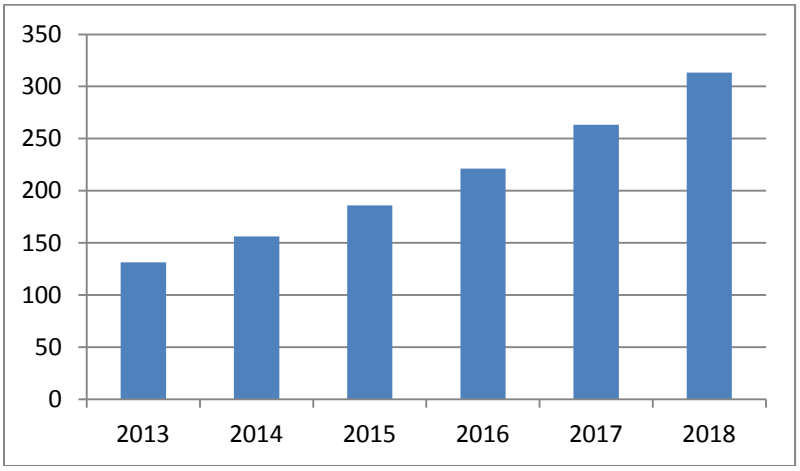

Exhibit 1
Firewall Analysis Market Forecast
Source: the Ogren Group

Executive Summary

Firewalls rely on IT-defined rules in allowing authorized application traffic to flow unencumbered between data centers and users while preventing undesirable traffic from entering the corporate network. These rules, which can number in the thousands per firewall, prescribe allow/deny decisions based on sources, destinations, and the services provided. The more complex the network, the more complex the firewall rule sets, and the more likely IT will encounter disruptive side-effects when changing firewall rules to secure application access.

The primary reason to analyze firewall rule sets is to identify logic errors opening security gaps, violating compliance policies for segmenting regulated data, preventing subsequent rules from firing, or rules becoming obsolete due to changes in business services. This leads to business benefits in managing network complexity such as:

- Drive operational costs out of making changes to firewall rule sets by reducing errors, automating compliance reporting, and recommending effective rules based on application requirements.
- Accelerate application deployment cycle times by streamlining firewall change processes to a matter of hours.
- Enable an orderly evolution to application-centric security management for next generation firewalls as well as traditional deployed firewalls.
- Model the impact of new rules before a change is approved to protect against errors that could block application paths.
- Maintain a secure audit log of firewall rules changes to document all changes for compliance reporting.

Firewalls connect businesses to the Internet. It is the one security technology that truly enables a stronger business by securing application paths to users. The Ogren Group believes it is critically important for organizations to apply technology to help manage accuracy and instill a change process to control operating costs with increasing complexity in networks and firewall rule sets.

It is far from certain that firewall analysis will be more than a niche market with room for multiple vendors. Firewall analysis vendors are branching into application security motivated by next generation firewall concepts, enterprise security management to reduce operational costs, and threat assessment based on path analysis. *The Ogren Group applauds AlgoSec for their vision and execution in Firewall Analysis.*

In this report, the Ogren Group presents the features, life cycle, and market strategy of Firewall Analysis. The report concludes with recommendations for enterprise buyers.

Overview

Firewall Analysis began with the value proposition that improving the efficiency of firewall rule sets would make firewalls easier to manage, firewalls would perform better, and the organization could postpone investments in firewall upgrades. The features found customer traction in organizations with complex networks, where organizations needed to normalize views of diverse firewall rule sets from multiple vendors (such as Cisco firewalls with fine-grained rules and Check Point with more encompassing rules), or needed automation to simplify adherence to compliance mandates.

The focus on rule sets provides organizations definitions of application paths based on actual firewall configuration settings, as opposed to those expected by security policy. The ability to analyze thousands of firewall rules and express the security implications of application access to its customers is the intellectual property of Firewall Analysis vendors and defines market participants.

First generation solutions had a revenue growth issue in that organizations, even though they were satisfied with the benefits delivered, viewed the technology more as a tactical tool to ne used a few times per year. The second generation of Firewall Analysis thus saw features aimed at encouraging daily use of the product capabilities, such as previewing recommended rules changes, managing auditable change processes and approval workflows, and tracing attack paths to locate vulnerable applications. Vendor price points and revenue streams improved as organizations incorporated Firewall Analysis into their standard operations best practices.

The Ogren Group believes that every organization reliant on keeping application paths clear and secure should be using Firewall Analysis in its daily operations. No organization should rely solely on the brain of a security expert to create rules without technical assistance and no organization should use spreadsheets to document firewall rule sets.

Firewall Analysis is undergoing a fundamental transition to incorporating application security, enterprise security management, or threat assessment features and the winners will be those successfully meeting the requirements of the market's economic and technical drivers.

Economic Drivers

Firewall Analysis is driven mostly by operational cost savings related to firewall rules administration, security requirements associated with complex networks, and compliance with regulatory mandates.

Network complexity is increasing to meet demands of application deployment "at the speed of business". Lines of business within organizations require new or upgraded applications to be launched in minutes or hours, which places pressure on security teams to create and deploy new firewall rules securing application access. The impact of urgent application deployment also increases the risk of disrupting the business due to errors in firewall rules.

Hiring limitations force organizations to reduce operational costs with technology. Global economic conditions, particularly uncertainty about future growth, have made it challenging to hire security professionals to manage increasing network complexity and application access demands. Enterprises apply Firewall Analysis to save time and operating expenses every time a firewall rule set is modified – which for many is a daily occurrence.

Best practices for compliance audits of government and industry regulations are becoming continuous. There are a number of firewall and access control requirements that are common among IT regulations such as PCI-DSS, HIPAA, and NIST. Firewall Analysis helps organizations meet these firewall configuration requirements in effective and cost-efficient ways, including:

1. A formal process for approving and testing changes to firewall configurations.
2. Restricting inbound and outbound traffic to regulated services to what is necessary.
3. Diagramming all network connections to regulated data.
4. Documenting use of all services, protocols, and ports allowed.
5. Building a firewall configuration restricting connections between un-trusted networks and regulated services.

Technical Drivers

In addition to economic drivers, Firewall Analysis requirements are also driven by technical drivers that are causing fundamental shifts in the way organizations manage and secure their networks:

Internal business applications, such as those found with e-commerce systems or large business management suites with complicated relationships between web servers, application engines, and data bases drive increasingly complex demands on secure access policies. Organizations are shifting to application-oriented security policies to improve communication and coordination between network, application, and security teams. This also creates demand for technology to help manage relationships between application requirements (that are no longer defined as external web sites) and firewall rules.

Next generation firewalls shift firewall rule set emphasis from source-destination-service to application-user. The explosion of application-centric firewalls, such as those from Palo Alto Networks, inspires IT to evolve towards new application-oriented administration while maintaining legacy firewalls. This disruptive evolution to next-gen firewalls provides an opportunity to insert Firewall Analysis into corporate security operations procedures to manage increased change requests.

Virtualization, including rapid application provisioning and application movement between data centers, mandates streamlining firewall rules procedures. Application paths through firewalls need to be efficiently kept clear to accelerate application deployment, eliminate the chance of errors creating application or network outages, and reduce the risk of security incidents. Business requirements drive greater efficiency in providing secure application access.

Threat successes force security teams to shift priorities to network-based configuration control technologies. Organizations increasingly recognize that they cannot control new threats designed to defeat anti-malware defenses, but they can require the network to discover and control vulnerable insecure configurations and exploitable vulnerabilities.

Noteworthy Features

Firewall Analysis features are derived from an ability to interpret application paths from firewall rule sets, understand the order of precedence when rules fire or can never be used, and map firewall rules to business requirements. The noteworthy features also include innovative functionality for application security, enterprise security management, and threat assessment.

Model the effect of suggested rules changes in "what if" scenarios. Organizations reduce error rates and the risk of creating security holes by evaluating recommended changes to rule sets before the changes are committed and deployed.

Recommend rules based on application connectivity requests. Security teams may enter the request for application connectivity in business terms and Firewall Analysis will go beyond

validating IT-supplied rules to actually recommend the firewall rules required to satisfy the request.

Record an audit trail of all changes to firewall rules sets. Automatically report on firewall change history, including requester of change, business justification, required application services, review and approval sign-offs.

Manage workflows to enforce review and approve steps in firewall rules change procedures. One large problem in firewall administration is an unauthorized change that has not been peer-reviewed. Firewall Analysis detects "out of process" changes to rule sets and notifies security teams if there is no corresponding workflow.

Identify rules that can never be used and are eligible for removal. Firewall Analysis detects unused rules that may be removed from rule sets without adversely affecting security. For example, firewall rules may be shadowed where the firewall abides by the first relevant rule it encounters (and never gets to subsequent specific rules that may overlap) or rules may refer to servers and applications that have been retired.

Import spreadsheet tables into Firewall Analysis management consoles. Organizations relying on spreadsheets to maintain and document changes to firewall rule sets place themselves at great risk of errors, security incidents, or non-compliance.

Translate firewall rule sets from multiple vendors for a common view of network security. Large organizations expect to have devices from multiple vendors, such as a combination of Check Point, Cisco, Juniper, and Palo Alto firewalls. Firewall Analysis assists firewall management by translating business and application requirements into rule sets for each vendor.

Trace paths from external sources to potentially reachable internal targets. Security teams need all of the help they can get in responding to new threats, and knowing which systems can directly connect to other systems may be critical information in reducing the risk of a security incident.

Integrate firewall rules changes into application provisioning procedures. Vendors incorporate custom workflow features or integrate with leading vendors such as Remedy to seamlessly connect security best practices with IT operations.

Enable migration to application-centric security management. Firewall Analysis not only helps organizations migrate rule sets to next generation firewall features, but also allows them to manage application paths by business rules more than source-destination-service constructs.

Noteworthy Weaknesses

While the Ogren Group believes Firewall Analysis provides critical functionality to organizations required to secure complex networks, there are noteworthy weaknesses that may keep this a niche market with a relatively few number of successful vendors.

Firewall analysis is viewed by many organizations as a tactical tool for quarterly or annual compliance assessment or firewall migration. The status quo usually is the toughest competitor, and some organizations use Firewall Analysis to meet short-term security needs only to return to the traditional process of manually managing firewalls with spreadsheets.

There is little performance return for the operational risk of culling obsolete rules. An early value proposition of Firewall Analysis was that removing unused rules from rule sets enhanced firewall performance and extended firewall lifecycles. However, some organizations feel there is not enough benefit in removing rules from firewalls that are otherwise working and performing adequately.

Firewall vendors are improving their ability to analyze rules. It is in the best interests of firewall vendors to make it easy to reflect business needs in their firewall rule sets. For example, Check Point's Compliance Blade is drawing interest from many organizations that may have been attracted to Firewall Analysis in Check Point environments.

Threat path analysis is of questionable value in protecting network resources. Attacks will penetrate firewall perimeters by finding security gaps, mimicking trusted services or using infected endpoints to reach network resources. *The Ogren Group finds organizations reduce the risk of disclosure events by assuming critical resources are exposed to all threats, regardless of threat paths or how many hops an attack must take before finding a vulnerable resource.*

Firewall Analysis is seen as a fit for large enterprises with complex networks and expensive security operations; a tougher fit for medium enterprises with fewer firewall operational expenses. Network complexity with a large number of firewalls and applications is a fundamental driver for Firewall Analysis technology, but that restricts the addressable market to larger enterprises.

Application Security-Centric Approaches

One of the sustaining IT trends is to manage by applications and users, rather than by managing source addresses, destination addresses and services (where services can no longer be reliably identified by port). Application security-centric Firewall Analysis vendors enable IT teams to communicate security policy needs by higher level application definitions and users which promises to deliver important benefits to enterprises:

- Application owners, network administrators, service desks, and security teams can all communicate requirements in application terms associated with business objectives. In fact, teams may share the same Firewall Analysis views for a more efficient coordinated process.
- Security policies can be more easily integrated into application provisioning procedures. For example, Firewall Analysis can check and ensure compliant application paths before IT launches a new application.
- Application security-centric Firewall Analysis can help security teams manage the complexity of large application environments that may be composed of combinations of web servers, application engines, databases, and networking equipment.

AlgoSec

AlgoSec was started in 2003 with headquarters in Boston, MA and engineering centered in Israel. The company was an early Firewall Analysis innovator and has persisted as a market leader in network security. In February 2013, AlgoSec announced 54% annual sales growth over the past three years, with more than 1000 customers world-wide.

A Fortune 50 manufacturing organization first used AlgoSec to cull 10% to 15% of its 40,000 rules that were not used within 90 days. The customer experience was positive, and the organization extended the use of firewall analysis to manage its daily process of changing rules within its 500 Check Point or Cisco firewalls. The organization states that saving IT time is the leading benefit of incorporating firewall analysis into its global technical deployment process, with meeting compliance requirements a close second.

BusinessFlow highlights AlgoSec's push into application security. The Ogren Group is impressed with the approach of defining the entire end-to-end application environment, with the presentation of application-oriented security views, and with the impact on the agility organizations require in managing complicated application environments.

AlgoSec's top product offerings include:

- *Firewall Analyzer* optimizes firewall rule sets, validates that proposed changes align with security policy, recommends changes to rule sets based on best practices, and tunes rule sets without adversely impacting business connectivity.

- *FireFlow* technology manages workflows associated with firewall rule change procedures, integrating firewall security management with network and IT management procedures.
- *BusinessFlow* is AlgoSec's innovative approach to allow security teams to administer network security based on application requirements. This is a powerful approach that simplifies managing network security settings for the entire application environment including web servers, application engines, and databases.

AlgoSec is has been a model performer in the Firewall Analysis market. The introduction of BusinessFlow significantly broadens AlgoSec's opportunities for enterprise level sales within large organizations. *The Ogren Group recognizes AlgoSec for their leadership in the Firewall Analysis market.*

Threat Assessment-Centric Approaches

Firewall Analysis intellectual property includes the ability to map possible network connections to internal resources based on what is allowed or blocked according to firewall rules. Vendors use threat path intelligence to detect vulnerabilities that are potentially exposed to externally-sourced exploits. *The customer benefit is that security teams can use this threat assessment to save time and effort by prioritizing mitigation efforts based on the probability of an exploit reaching a vulnerable resource, and by ensuring that security filters are deployed on every threat path to sensitive resources;* the vendor benefit is the ability to tap into threat prevention items of the security budget which is substantially larger than that allocated to firewall management.

The Ogren Group believes that security teams should always assume that an exploit will find a critical vulnerability in a critical resource and should aggressively patch and upgrade software to mitigate the risk of a security incident – regardless of the degree of difficulty shown by threat assessment features. Use Firewall Analysis threat assessment to find unprotected network segments, test regulated security zones for compliant access controls, and focus incident response processes to track the spread of an attack.

Enterprise Security Management-Centric Approaches

The leading benefit of Firewall Analysis is operational cost savings, a benefit that was consistently mentioned before compliance or enhanced security. New entrants into Firewall Analysis are taking the approach of integrating firewall rules management into enterprise security management procedures.

Enterprise Recommendations

The Ogren Group believes that all organizations with complex or high performance networks should be using firewall analysis technology to automate rule change procedures for cost savings, attest that compliance with security policy is maintained before committing to rules changes, and assure that security holes are not created with ineffective firewall rules. Organizations rely on firewalls to establish secure application paths to users, and Firewall Analysis is critical to save time and energy in keeping those application paths clear.

Ogren Group recommendations to enterprises include:

Identify firewall rules that have not been used within 90 days in proof of concept efforts. Most organizations are surprised that deployed firewall rule sets inadequately reflect actual application requirements. An early measure of the quality of firewall rule set is the number of rules that have not been used within a full business quarter.

Build in time and quality measurements as part of your proof of concept effort. While Firewall Analysis has definitive security benefits, its primary benefits are saving time and effort in firewall management. Evaluate the technology for time saved creating rules changes, reducing the error rate, generating compliance audit reports, reducing unauthorized changes, or tracing threat paths to possibly infected systems.

Institutionalize use of Firewall Analysis as a critical element of firewall rules change procedures. This is a no brainer – use the interfaces of Firewall Analysis to automate firewall rule change workflows, model the impact of change requests before they go live, and create documented audit trails of rules changes and business justifications.

Evaluate application-oriented firewall management. The Ogren Group recommends that organizations investigate application-oriented Firewall Analysis to enhance coordination between application, network, and security teams, to integrate secure access into application provisioning, and to help security manage security requirements for complicated application environments.

Use the evolution to next generation firewalls to deploy Firewall Analysis. Next generation firewalls may induce more firewall change requests and the need to map application-centric concepts onto traditional firewalls. The Ogren Group suggests that organizations evaluate Firewall Analysis as part of their program to incorporate next generation firewalls.

Market Directions and Predictions

The Firewall Analysis market will grow at a steady 19% CAGR through 2018. Market growth depends on trends in next generation firewalls, traditional firewalls, and the ability of Firewall Analysis vendors to demonstrate substantial operational cost savings.

Half of the major Firewall Analysis vendors will be acquired by network management vendors by the close of 2014. The Firewall Analysis market as defined has too many vendors competing for business. The Ogren Group predicts fully half of the existing vendors will be acquired by the close of 2014.

Evolution to application security, particularly for next generation firewalls will dominate Firewall Analysis customer requirements. Organizations loathe investing in legacy firewalls that have been performing adequately for years. Firewall Analysis demand will increase with its ability to facilitate secure deployment of applications and to manage network security with an application-centric view. The Ogren Group expects application security requests to monopolize vendor requirements.

Conclusions

The Ogren Group believes that all organizations with complex or high performance networks should be using firewall analysis tools to attest that compliance with security policy is maintained before committing to rules changes, assure that security holes are not created with ineffective firewall rules, and remove obsolete rules that may adversely affect firewall performance. Interviews with enterprise security professionals relate that automating firewall rule change procedures yields significant cost savings, driving deeper vendor penetration into customer organizations.

A key go to market strategy for Firewall Analysis is to capture new business, even with small deal sizes, and then grow the account once they appreciate the benefits of Firewall Analysis. Most vendors also plan to upsell the installed base to products oriented to application security, enterprise security management, or threat assessment. The Ogren Group believes that application security offers the most revenue potential as that meshes with next generations of firewalls and business strategy while maintaining the vendor focus on security; enterprise security management offers deeper cost savings potential for organizations integrating security and IT administration; threat assessment is a questionable approach to protecting the network against zero-day attacks.

In all cases, however, Firewall Analysis saves organizations time in keeping application paths clear. The Ogren Group highly recommends security teams evaluate Firewall Analysis within their organization.

The Ogren Group has licensed this report to AlgoSec for unlimited, unedited distribution. This is a special condensed version of the *Firewall Analysis Saves Time Keeping Application Paths Clear* security report provided compliments of AlgoSec. No new text has been added – the condensed report focuses on AlgoSec with references to other vendors removed.