WHY BUSINESS APPLICATION VISIBILITY IS ESSENTIAL FOR YOUR NETWORK SECURITY POLICY MANAGEMENT

An AlgoSec Whitepaper

Executive Summary

The case for network security policy management is understood and accepted, and there is a clear trend of enterprises investing in this technology. However, is there more that enterprises can do to protect their networks and datacenters against security threats? Can increased visibility into business application usage help to identify additional security holes that can threaten the organization's security, agility or compliance posture?

This whitepaper examines the case for taking an application-centric approach to security policy management, to achieve and maintain a more secure network environment.

The Current Situation

The current setup in most organizations is an IT department comprised of different teams including networking, security, operations and others, each of whom are focused on their specific roles in addition to ensuring that all systems run smoothly.

On any given day, new business applications are added, changed or removed, which requires the implementation of complex, time-consuming network security changes. Furthermore, the current trend towards migrating business applications to the cloud brings its own trials and tribulations, including understanding the network connectivity of the said applications prior to deployment, provisioning the relevant firewalls and routers in the cloud, and then migrating and adjusting existing network connectivity to support them.

Moreover, for each business application to run smoothly, all teams within IT need to collaborate, align and communicate their needs in a common language, and one way to achieve this is to take the application-centric approach to security policy management.

An application-centric approach manages security policies from the perspective of the business applications that they support, in addition to the networking attributes used to enforce them.

The AlgoSec Security Policy Management Solution

The AlgoSec Security Policy Management Solution is the leading provider of business-driven security management solutions, helping the world's enterprise organizations to become more agile, secure and compliant. Comprised of a suite of three fully integrated products; AlgoSec Firewall Analyzer, AlgoSec FireFlow and AlgoSec BusinessFlow, the AlgoSec Security Policy Management Solution provides holistic, business-level visibility through a single pane of glass, across the entire network infrastructure.

With AlgoSec, users can automatically discover and migrate application connectivity flows, proactively analyze risk, tie cyberattacks and vulnerabilities to business processes and intelligently automate time-consuming security changes through easy-to-use workflows— all with zero-touch, and seamlessly orchestrated across the enterprise's cloud, SDN and on-premise network.

AlgoSec Firewall Analyzer delivers visibility and analysis of complex network security policies across on-premise and cloud networks, enabling optimization in configuring firewall routers web proxies and related network infrastructure, and ensuring security and compliance.

AlgoSec FireFlow facilitates automated security policy changes, saving time, avoiding manual errors and reducing risk. With FireFlow users can process firewall changes with zero-touch, assess the impact of network changes to ensure security and continuous compliance, automate rule recertification processes, and automatically document the entire change management lifecycle.

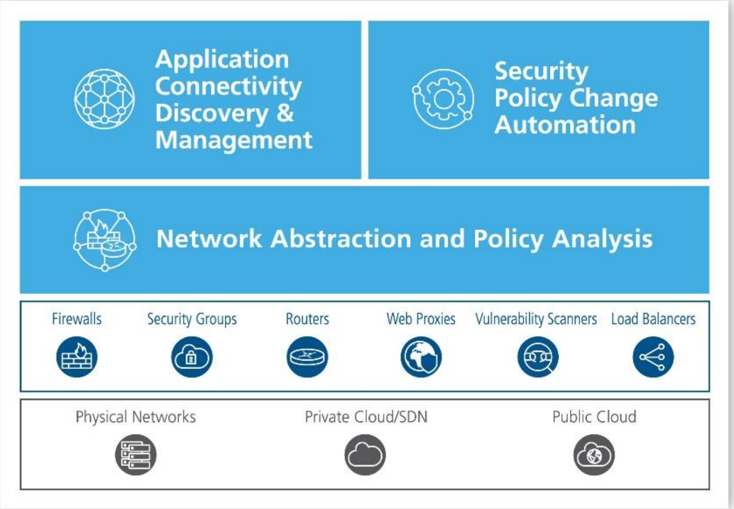

Fig 1. The AlgoSec Security Policy Management Solution

AlgoSec BusinessFlow enables users to manage network security from the business application perspective. BusinessFlow automatically discovers, and then provisions or securely decommissions network connectivity for critical business applications through easy-to-use workflows. BusinessFlow ties vulnerabilities to the applications impacted, to accelerate business application migrations to the cloud, avoid outages and ensure application security and compliance across virtual, cloud and physical networks.

The Case for Deploying AlgoSec BusinessFlow with AlgoSec Firewall Analyzer

When getting started with a network security policy management solution such as AlgoSec, customers are often faced with the dilemma of deciding how and when to deploy the different functionality. Their decision will be based on several factors including their perceived need, budget and work methodology.

Many customers prefer to take a cautious approach, and start with AlgoSec Firewall Analyzer to gain insight into their complex network security policies. As a result, they may not realize the benefits derived from deploying AlgoSec BusinessFlow at the same time.

The case for deploying AlgoSec BusinessFlow together with AlgoSec Firewall Analyzer is great. Through this deployment approach, all business applications are discovered, identified and mapped, providing visibility of the network connectivity flows associated with each business application, which in turn provides critical security information regarding the firewalls and firewall rules supporting each connectivity flow.

This deployment combination takes up to 4 weeks[1], and customers can begin to enjoy the benefits almost immediately, including:

Application-Centric Visibility: Full visibility of network security including application network connectivity flows, firewalls and the firewall rules that determine network traffic. This facilitates a deep understanding of the implications of any planned changes to application connectivity and how to configure the firewalls in line with these changes.

Another benefit of application-centric visibility is that it enables organizations to identify unknown or unused applications on their network. Statistics show that on average, 25% of business applications running in any organization are either unknown or shelfware. This lack of visibility can lead to security holes because network connectivity paths are left unmonitored.

Enhance Compliance: Having full knowledge of all business applications aids the company in their adherence to different compliance requirements. For example, PCI-DSS requires customers to audit all the applications that fall within the scope of the regulation. This information is easy to determine through application network connectivity mapping.

Accurate Planning: When planning a migration to the cloud or another data center, it is critical to understand the application's existing connectivity flows prior to migration, so that they can then be accurately adjusted to the new network architecture. This is especially critical if the migration is to a cloud platform.

[1] With the AlgoSec Jumpstart Package 1

Accelerate Troubleshooting: Application network connectivity mapping can reveal whether an application outage is due to issues with the network. For example, an employee opens a support ticket when he's not able to connect to the CRM application. Typically, the ticket will first go to the network team to determine if the problem is network related. Using the application-centric approach with its associated mapping, it is immediately clear whether the issue is network-related. If it is, it can be easily dealt with. If not, it can be sent to the appropriate department, without wasting time and resources.

Impact analysis: Application network connectivity mapping provides a clear picture of the impact on business applications, of any planned changes to the network. This can include firewall changes, or other changes that may cause network downtime. Mapping will enable the implications of the changes to be fully understood and consequently, downtime, for example, can be scheduled for when it will have minimum impact on customers, partners, or employees, i.e. not during office hours.

Assess and Prioritize Vulnerabilities: Viewing network vulnerabilities from a business application perspective enables organizations to immediately assess their impact on the business and prioritize remediation efforts based on business and security priorities.

Collaborative Teamwork: Speaking in "business application terms" will help to bridge the gaps between the IT teams and the application delivery teams, and enable application, security, networking, risk and cloud experts to collaborate using the same language.

Summary

The three products that make up the AlgoSec network security policy management suite; AlgoSec Firewall Analyzer, AlgoSec Fireflow and AlgoSec BusinessFlow are integral and critical components of a comprehensive network security policy management solution. While the greatest benefit is derived from deploying all three products from the outset, some customers may prefer to take a staggered approach to deploying them, based on their immediate needs, budget and work methodology.

Many companies choose to focus initially on firewall policy analysis (using AlgoSec Firewall Analyzer) and then proceed to automating changes to their network policy (using AlgoSec FireFlow) and lastly, add the business application perspective (using BusinessFlow). This approach, while legitimate, does not allow customers to gain full visibility into their business applications and network connectivity flows, and this lack of network information leaves the network vulnerable and open to security holes.

An alternative approach, would be to deploy AlgoSec Firewall Analyzer and AlgoSec BusinessFlow together from the outset, to achieve maximum visibility of the network and its associated business applications. This approach enables the customer to seamlessly identify network security holes and vulnerabilities, plan and enable a seamless migration to the cloud, accelerate troubleshooting while simultaneously adhering to the highest compliance standards.

To discover more about Algosec's business-driven security management solution, visit www.algosec.com, or click here to request a demo.

About AlgoSec

The leading provider of business-driven security management solutions, AlgoSec helps the world’s largest organizations align security with their business processes. With AlgoSec, users can discover, map and migrate business application connectivity, proactively analyze risk from the business perspective, tie cyber-attacks to business processes and intelligently automate network security changes with zero touch - across their cloud, SDN and on-premise networks. Over 1,500 enterprises, including 20 of the Fortune 50, utilize AlgoSec’s solutions to make their organizations more agile, more secure and more compliant - all the time. Since its inception, AlgoSec has provided the industry’s only money-back guarantee.

Global Headquarters
65 Challenger Road,
Suite 320
Ridgefield Park
NJ 07660, USA
+1-888-358-3696

EMEA Headquarters
80 Coleman Street
London EC2R 5 BJ
United Kingdom
Tel: +44 207-099-7545

APAC Headquarters
Centennial Tower, Level 21
3 Temasek Avenue
Singapore 039190
Tel: +65 6549 7415

AlgoSec.com