SECURITY POLICY MANAGEMENT ACROSS THE NEXT GENERATION DATA CENTER

An AlgoSec Whitepaper

MANAGE SECURITY **AT THE SPEED OF BUSINESS**

Introduction

Corporate networks today must deliver hundreds of mission-critical business applications and be flexible enough to support productivity innovations “at the speed of business”, all while preventing cyber-attacks and ensuring compliance. If that weren’t challenging enough, the enterprise network environment itself is evolving rapidly as companies extend their physical data centers to embrace cloud computing and software-defined networking in order to take advantage of the flexibility and cost-savings these environments offer.

As a result, the security policy that protects the organization has become bigger and more complex than ever before—outstripping the ability to manage it manually. This whitepaper examines the new reality facing today’s security, networking and application teams, the challenges of managing the security policy in an environment of constant change and complexity, and the solutions that can help manage security at the speed of business.

Understanding the Challenges

More Applications and More Complexity

In a recent survey AlgoSec found that 32% of respondents managed more than 100 critical data center applications, while 19% oversaw more than 200. These applications typically require a complex multi-tiered, distributed and interconnected architecture and elaborate communication paths across other applications, servers and databases – on-premise and in private and public clouds. Additionally this enterprise infrastructure requires more firewalls, more encryption and more points of authentication than ever before – placing even more demands on the networking and security teams.

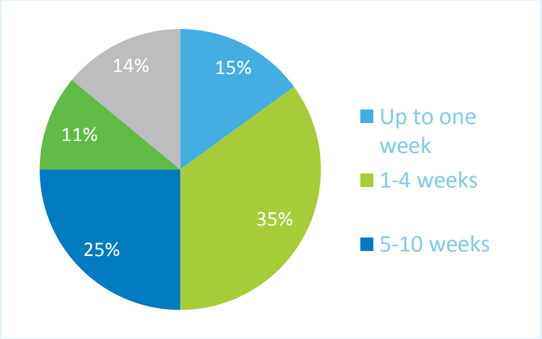


Figure 1: Average time to deploy new data center applications. From “Examining the Impact of Security Management on the Business” AlgoSec Survey.

The network and security teams can’t “just” manage the 100+ applications they have at any one time and consider themselves done. There are constant upgrades and changes, and new applications to deploy, connect and secure as business users demand that they be up and running as fast as possible.

Consequently, as the AlgoSec survey found, it takes over a third of companies more than 5 weeks to bring a new application online and nearly 60% of companies report that it takes more than eight hours to process an application connectivity change.

More costly threats

As the growing number of complex applications increases the pressure on IT, so too has the sharp rise in the number of high visibility and costly data breaches. According to a recent PwC survey the average data breach costs a large enterprise $5.9 million, making security a top concerns for executives, regulators and the board.

To protect the network and critical data from both internal and external threats, many organizations have adopted a defense-in-depth strategy, network segmentation or both. The defense-in-depth approach layers security controls to block access at multiple points, while the network segmentation approach isolates sensitive data and key devices in separate zones which are protected with specialty firewalls and a variety of choke points. Whether an organization uses a defense-in-depth or network segmentation strategy, the increased security means more network devices, more complexity and more management headaches for IT.

More cloud computing

To meet the demand for speed, capacity and reduced costs, many enterprise organizations are beginning to utilize cloud platforms for business applications.

While two-thirds of organizations recently surveyed by AlgoSec had deployed or expected to deploy business applications on a public cloud platform within the next 36 months, the majority stated that extending their corporate security policy to the public cloud poses significant challenges. 80% said they needed greater visibility across their on-premise and public cloud environments, and most companies have little idea what security controls they need, and how to incorporate and manage them across their hybrid environments.

Even as IT worries about cloud security issues, business application owners and developers often embrace the cloud under the radar of the security and networking teams. This “shadow IT” increases corporate vulnerability and puts the IT department in the position of being responsible for mitigating risks for applications it doesn’t even know exist. To shut down shadow operations, IT must evolve from being the bottleneck department to becoming a business enabler that quickly responds to users’ requests while maintaining security.

Addressing Security Policy Management Challenges

Provision connectivity for data center applications

As new applications are added — or the connectivity requirements for existing ones are modified — network operations and security administrators must be able to assess the underlying firewall rules and changes that are needed, and initiate the correct change management workflow for implementation.

However, application connectivity requirements are rarely documented, let alone maintained, with many organizations relying on spreadsheets, seldom-updated databases, and team members' memories for this information. This makes meaningful discussions about required changes with application owners and others - who don't typically speak in the language of ports and protocols - near impossible.

Adopting an application-centric approach to security policy management will enable organizations to overcome these challenges. Application-centric analysis that is fully integrated in a security management solution can automate the change workflow and address common challenges such as:

- Identifying the impact of proposed network changes, such as server migrations or new routing and segmentation schemes, to the organization's applications.
- Accurately identifying/removing access rules for decommissioned applications, without impacting the accessibility of other applications.
- Determining the impact of proposed changes to access rules — for example, in response to newly discovered threats or vulnerabilities — to an organization's applications.
- Using application connectivity requirements as a layer of abstraction to help mask the growing complexity of today's security policies.
- Bridging the communication gaps between the different constituencies within IT.

Keep up with changing business requirements

Business requirements change at breakneck speed in today's global environment, and the organization's business applications and their underlying connectivity must be adjusted accordingly in order to support business needs, while maintaining the security posture and reducing risk.

Given the sheer complexity of the network and security infrastructure, failure to properly manage changes can lead to outages, as well as security and business risks. Factors that contribute to this problem include:

- Lack of formal processes for change management
- Poor communication between key stakeholders
- Lack of understanding of relevant business risks

Effectively managing security changes requires an automated and application-centric solution in conjunction with formal processes. Organizations must have well-defined, documented policies and procedures, backed into automated technical controls that provide visibility, management and enforcement. Standardizing and automating the security policy management process also makes the change management process go much more smoothly – and ensures that everyone's on the same page instead of assuming they know what other groups want or need. Ultimately by automating much of the security change management process reduces errors and risks and allows IT to respond "at the speed of business," not 11 weeks later.

Understand risk in the business context

With recent breaches making front page news, security is now a top priority for business stakeholders. To address this, security leaders and their teams must come up with ways to make business stakeholders aware and accountable for IT security risks in their business units.

But traditional risk management practices typically have a very technical focus, displaying risks for servers, IP addresses, and other elements that are somewhat meaningless to business managers. Here too, organizations would be wise to adopt an application-centric approach, associating and prioritizing risks with a line of business.

One method is to integrate security policy management with vulnerability scanners that are already in use in the organization. Organizations can map vulnerabilities with their related data center applications, including their servers and complex connectivity requirements. Vulnerabilities and severity can then be scored across each application server and aggregated per application to provide a holistic view of the business risk. As application connectivity flows change, these scores should be updated to ensure a current view of the application risk at all times.

Simplify audits and ensure continuous compliance

More than 400 regulations with 10,000 overlapping controls govern network security worldwide. In addition, organizations have their own internal standards as well as those established with partners, customers and the industry.

Typically, many organizations must undergo multiple audits every year, which can significantly drain a company's IT resources. Almost three-quarters of respondents to an AlgoSec survey reported that they spent more than one man-week on firewall audits annually and 17% said firewall audits consumed more than one man-month each year. Solutions that provide visibility into the network and applications and enable companies to audit, prove and document their security or compliance status at any given time make the auditing process far easier and less time consuming.

Maintain an optimized network security policy

When an application is deployed, the security team defines access rights and creates firewall rules. When an application is decommissioned, the reverse seldom happens. This leads to cluttered policies, which in turn can slow down firewall performance and make it difficult to troubleshoot connectivity issues. Most importantly, it can leave open doors that expose the organization to risk. An automated security policy management solution that shows the network topology and presents an analysis of traffic and network access flows by application can quickly identify unused, unnecessary, overly permissive and duplicate rules as well as connectivity problems caused by specific firewalls.

Unify security policy management across hybrid cloud data centers

Organizations increasingly look to extend their on-premise data centers to public cloud Infrastructure-as-a-Service (IaaS) platforms to maximize business agility and reduce costs. But ensuring network access in the public cloud is a significant challenge due to the fragmented variety of cloud network security controls and the lack of visibility across the hybrid environment.

Moreover, the same on-premise network security management challenges—misconfigurations, manual and error-prone change management processes, and compliance, to name a few—must be addressed in the public cloud environment too. Solutions that extend visibility and can unify and automate security policy management across the hybrid data center are therefore more critical than ever before.

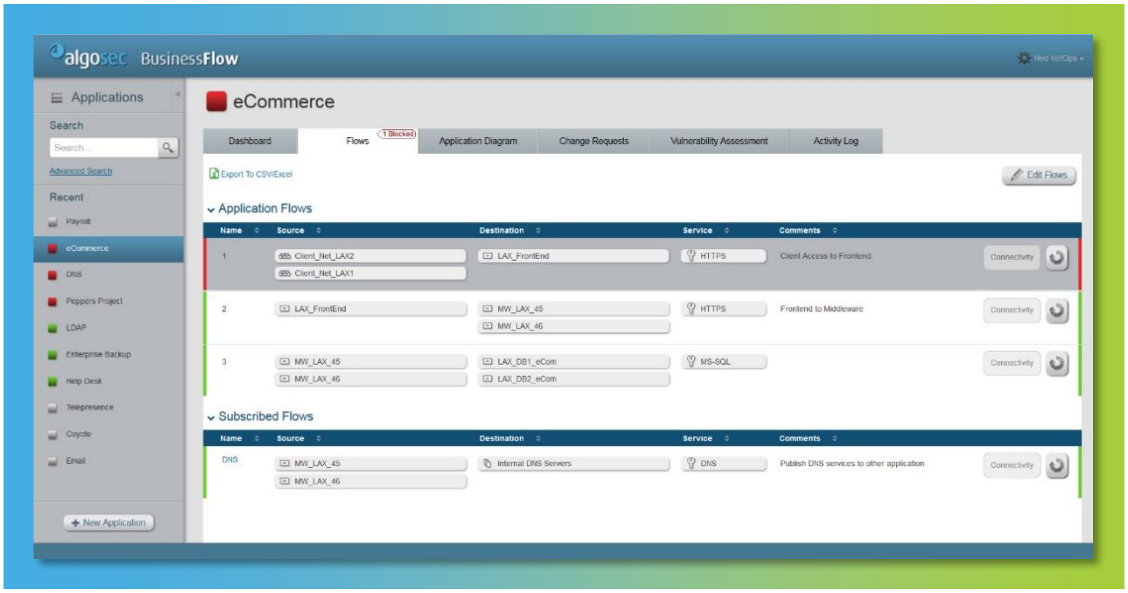
Improve Security, Compliance and Business Agility

The AlgoSec Security Management Solution manages complex network security policies throughout their lifecycle— from application connectivity discovery and migration, through ongoing change management and optimization to secure decommissioning. With powerful visibility across firewalls and cloud security controls, AlgoSec simplifies, automates and orchestrates security policy management to accelerate application delivery while ensuring security and continuous compliance across the enterprise.

AlgoSec Benefits	Why use AlgoSec?
• Quickly and securely provision application connectivity, and avoid outages	• Security policy change management
• Unify security management across heterogeneous cloud, software-defined and on-premise environments	• Firewall policy optimization
• Automate the entire firewall change management lifecycle and eliminate misconfigurations	• Application connectivity management
• Deliver an optimized security policy that provides you with better protection against cyber-attacks	• Application and data center security migration
• Reduce time and costs of your firewall audits by 80% or more	• Hybrid cloud security management
• Self-document your entire security policy change lifecycle	• Firewall auditing and compliance
• Align your security, networking and application teams, and foster DevSecOps	• Risk impact assessment

Provision application connectivity with AlgoSec

AlgoSec makes it easy to securely provision, maintain and decommission connectivity required by business applications. By automatically mapping application connectivity requirements to the underlying network infrastructure, AlgoSec accelerates application delivery, minimizes outages and enforces security and compliance across virtual, cloud and physical data centers.



eCommerce

Application Flows

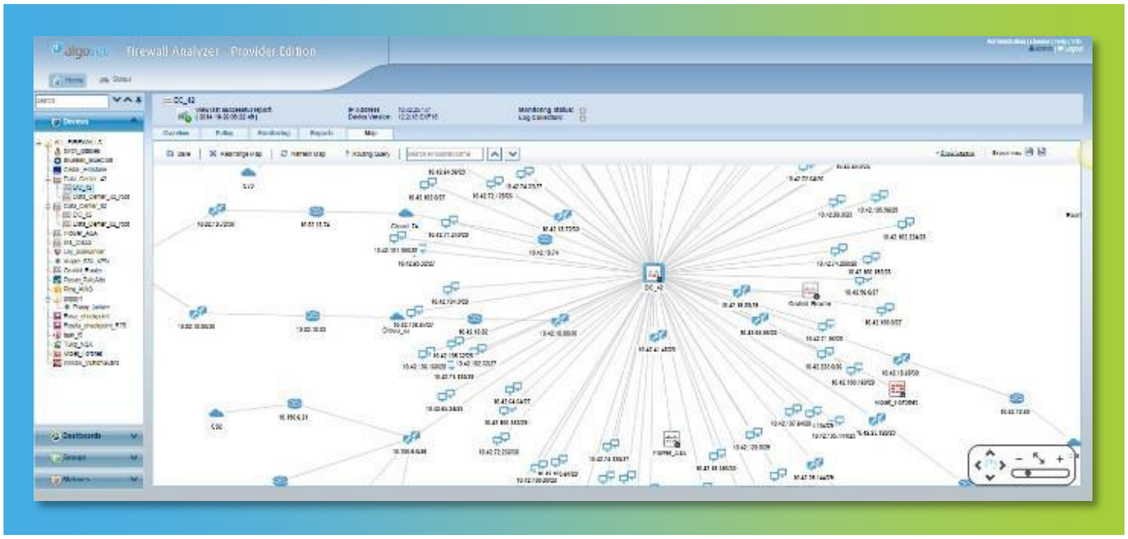
Name	Source	Destination	Service	Comments
1	Client_Net_LAX2 Client_Net_LAX1	LAX_FrontEnd	HTTPS	Client Access to Frontend.
2	LAX_FrontEnd	MW_LAX_45 MW_LAX_46	HTTPS	Frontend to Middleware
3	MW_LAX_45 MW_LAX_46	LAX_DB1_eCom LAX_DB2_eCom	MS-SQL	

Subscribed Flows

Name	Source	Destination	Service	Comments
DNS	MW_LAX_45 MW_LAX_46	Internal DNS Servers	DNS	Publish DNS services to other application

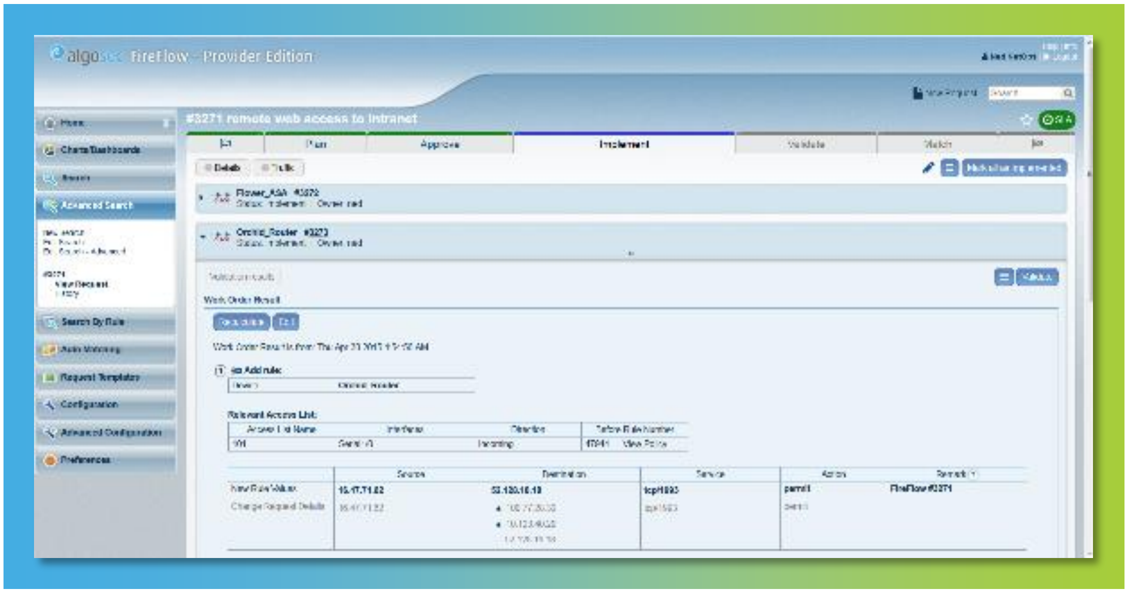
Visualize and analyze complex network security policies with AlgoSec

AlgoSec delivers visibility and analysis of complex network security policies across physical, virtual and cloud environments. It automates and simplifies security operations including troubleshooting, auditing and risk analysis. Using AlgoSec, security and operations teams can optimize the configuration of firewalls and routers, as well as related network infrastructure, to ensure security and compliance.



Automate security policy changes with AlgoSec

AlgoSec automates the entire security policy change process — from design and submission to proactive risk analysis, implementation, validation and auditing. By eliminating guesswork though intelligent change management workflows, AlgoSec helps operations and security teams save time, avoid manual errors and reduce risk.



#3271 remote web access to intranet

Flower_ASA #3272
Status: Implement Owner: [illegible]

Orchid_Router #3273
Status: Implement Owner: [illegible]

Work Order Result

Work Order Results from: Thu Apr 23 2015 [illegible] AM

1 Add rule:

Device	Orchid_Router

Relevant Access List:

Access List Name	Interface	Direction	Before Rule Number
101	Serial0/0	Incoming	47941 View Policy

	Source	Destination	Service	Action	Remark
New Rule Values	10.47.71.82	53.120.10.10	tcp/1893	permit	FireFlow#3271
Change Request Details	10.47.71.82	[illegible]	tcp/1893	permit	

About AlgoSec

AlgoSec simplifies, automates and orchestrates security policy management to enable enterprise organizations and service providers to manage security at the speed of business. Over 1,500 of the world's leading organizations, including 15 of the Fortune 50, rely on AlgoSec to optimize the network security policy throughout its lifecycle, to accelerate application delivery while ensuring security and compliance. AlgoSec is committed to the success of each and every customer, and provides the industry's only money-back guarantee.

For more information visit http://www.AlgoSec.com or visit our blog.

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

AlgoSec.com