algosec | BUSINESS-DRIVEN SECURITY MANAGEMENT

Securely Managing the Hybrid Cloud with AlgoSec

EBOOK

Table of Contents

Introduction

In the past, all of your data was secured behind lock and key, guarded by physical firewalls in locations that you could physically access. Now, your network is far more complex. It extends beyond the traditional perimeter, sitting in multiple locations and geographies

The typical medium or large enterprise now manages a dynamic heterogeneous (also known as hybrid) network that includes:

- On-premise data centers
- Public clouds - The most popular public clouds, AWS and Microsoft Azure, have become part of the computing fabric of millions of enterprises.
- Private clouds - Typically an SDN (Software-Defined Network) fabric that allows organizations to securely and efficiently host workloads on-premises.

These networks are complex, with multiple layers of security controls. On-premises data centers have network firewalls, routers and load balancers, frequently from a variety of vendors. Public clouds add their own security controls, such as cloud-native security groups, cloud-vendor advanced firewalls, and third-party firewalls by firewall vendors such as Check Point CloudGuard, Palo Alto Networks VM-series. Private clouds have their own security controls, such as Cisco ACI contracts and VMware NSX distributed firewalls. The proliferation of security controls in hybrid environments multiplies policy-management complexity and makes security policy management difficult.

IDC estimates that nearly **90%** of IT organizations will rely on a mix of on-premises/dedicated private clouds, several public clouds, and legacy platforms to meet their infrastructure needs.
In an AlgoSec/Cloud Security Alliance study, more than 2/3 of respondents also reported using multi-clouds.

Many organizations want to utilize the benefits offered by the public and private cloud, but stumble across **migration** challenges. They want to properly migrate their workloads to the cloud without compromising their security, while avoiding downtime.

Even in the on-premises world, traditional network security policy management within a single environment is challenging. Multiple firewalls from different vendors, thousands of rules and hundreds of weekly or monthly changes call for their careful management and automation. But as the network estate becomes even wider and more complex, coherent security policy has to extend across the entire heterogeneous network.

Network Security Challenges and Solutions

Running applications across the hybrid network can prove eminently useful for business teams but extraordinarily challenging for security teams. The complexity of the heterogeneous environment introduces a new level of security policy management challenges.

Visibility

The Challenge

You can't protect what you can't see. Visibility is essential to security and rapid incident response. Obtaining full visibility across the entire hybrid network requires a deep understanding of the hybrid network's topology and its traffic flows. Across your network landscape, security teams find it difficult to obtain a clear picture of your entire network. Enterprises find it difficult to have full policy and network visibility for their hybrid, multi-cloud environment, which are running different security and network elements, such as security groups, VPC routers and cloud firewalls. They don't know what the entire network topology looks like and how it works together. Tracking the operations, assets, and security controls across the hybrid cloud is challenging. Your security teams and business teams don't speak the same language, because you may lack visibility into the network connectivity flows associated with each business application.

In an AlgoSec/Cloud Security Alliance study,

39%
of respondents reported that the lack of visibility into the public cloud environment was a major barrier to cloud migration.

The Solution

With AlgoSec's security policy management solution, get a full network map of your entire hybrid network estate. AlgoSec delivers visibility and analysis of complex network security policies across your on-premises network as well as your cloud assets and security controls. AlgoSec analyzes and automatically discovers devices on your network and creates a virtual map of your network topology. The information is updated upon any device changes. It enables you to manage next-generation firewall policies and cloud security groups alongside traditional firewalls.

In the public cloud, AlgoSec also provides visibility for your cloud assets.

Managing Application Connectivity

The Challenge

The growing body of applications requires a complex, multi-tiered, distributed and interconnected architecture supported by elaborate communication paths that cross other applications, servers, and databases.

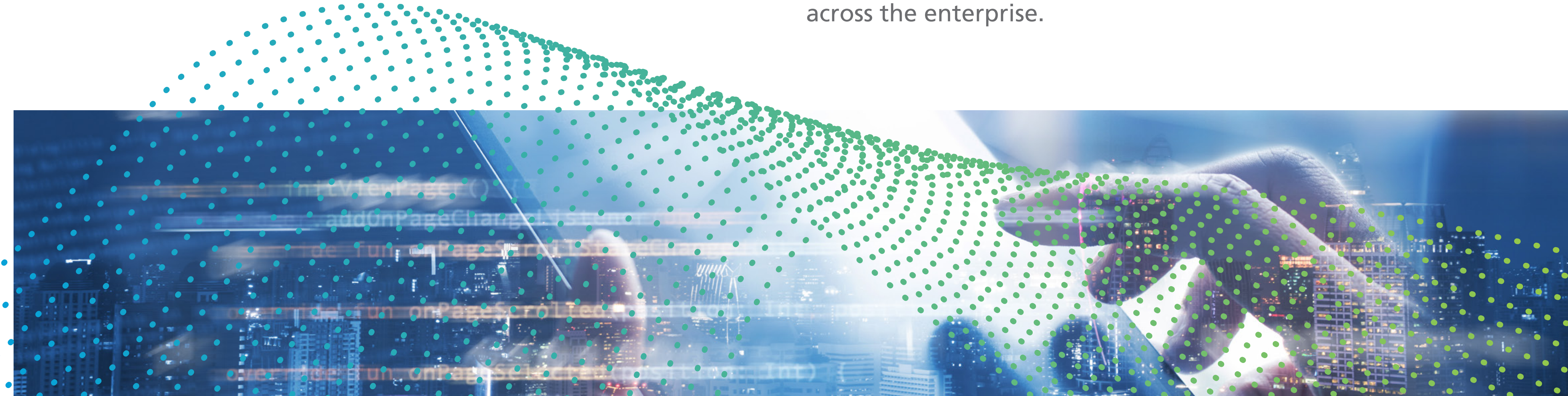
Trying to manage application connectivity across on-premise, private and public clouds, each with security controls by multiple vendors, is immensely complex and hard to gain control of. Business application owners and IT and security teams frequently don't speak the same language and so change requests are not fully understood, resulting in missed SLAs, outages, and misconfigurations.

The Solution

With AlgoSec you can discover, migrate, provision, change and securely decommission connectivity for business applications. AlgoSec automatically discovers and maps application connectivity requirements to the network infrastructure, and then translates requests for connectivity changes into networking terms that security and operations teams can understand, approve, and implement.

These capabilities allow streamlined and secured migration from on-prem to the cloud (private or public) without the fear of a downtime.

By understanding application flows, AlgoSec helps avoid network-related outages throughout data center migration or consolidation projects and enforces security and compliance across the enterprise.



Change Management

The Challenge

Making changes to the hybrid network security policy is a manual, complex, and error-prone process which slows down your business. Mistakes are common – and they cause rework, compliance violations, misconfigurations, and application outages. To add to the complexity, the change process involves multiple different devices across the hybrid network, as well as multiple teams, including security, networking and application delivery, who all have different objectives and communicate using different terminology.

Did you know?

With AlgoSec you can accurately process security policy changes in minutes or hours, not days or weeks.

The Solution

Using intelligent, highly customizable workflows AlgoSec streamlines and automates the entire security policy change process — from planning and design to proactive risk analysis, implementation on the device, validation and auditing. As part of the process, AlgoSec provides smart change recommendations for the security controls across the hybrid network, and can even provide zero-touch automation, implementing the changes across your network. Every step of the change process is fully documented to track accountability and SLAs, as well as provide a complete audit trail for your auditors. With AlgoSec, you will avoid guesswork and errors, reduce risk and complexity, enforce compliance, align teams and foster a collaborative approach to security policy management.

Maintaining Compliance Posture Management

The Challenge

Preparing your security controls for a regulatory or internal audit is a tedious, time-consuming and error-prone process. Moreover, while an audit is typically a point-in-time exercise, most regulations require you to be in continuous compliance, which can be difficult to achieve since your rule bases are constantly changing. With thousands of rules and ACLs across many different security devices, network environments, and numerous changes every week, it's no wonder that manually preparing for an audit has become virtually impossible.

The Solution

With AlgoSec, you can simplify security controls audits and ensure continuous compliance.

AlgoSec does all the heavy lifting for you. It automatically identifies gaps in compliance, allows you to remediate them and instantly generates compliance reports that you can present to your auditors. Additionally, all firewall rule changes are proactively checked for compliance violations before they are implemented, and the entire change approval process is automatically documented, enabling you to ensure continuous compliance across your organization.

Identifying and Remediating Risks

The Challenge

In hybrid networks, many network changes have taken place over time. These changes will be implemented on all the devices that direct traffic and are performed by the multiple stakeholders involved.

These changes may inadvertently introduce risk. The risks within the complex hybrid-cloud estate are too numerous and complex to be manually identified. There may be risks associated with business applications, duplicate, expired, or risky and overly broad rules.

The Solution

AlgoSec allows you to instantly assess, prioritize and mitigate risks in firewall policies, and map them to their respective business applications, to deliver a business-driven view of risk. AlgoSec checks your policy against an extensive database of industry best practices, which can be enhanced and customized with risks specific to your organization. AlgoSec also proactively assesses the risk of every proposed firewall rule change before it is implemented so that you can ensure that your policy remains secure and compliant all the time.

In the public cloud, AlgoSec CloudFlow lets organizations proactively detect misconfigurations to protect cloud assets, including cloud instances, databases, and serverless functions. Identify risky rules and their last usage date to gain the comfort to remove them so that you can avoid data breaches and improve your overall security posture.

Unwieldy and Risky Rules

The Challenge

Maintaining a clean set of firewall rules is a critical network-management function. In either the on-premises data center as well as in the cloud, applications are frequently commissioned and decommissioned. As firewall rules and cloud security groups are constantly adjusted, they can rapidly bloat. This makes it difficult to maintain, increasing potential risk.

Unwieldy rulesets are not just a technical nuisance. They also introduce business risks, such as open ports, unneeded VPN tunnels and conflicting rules that create the backdoor entry points that hackers love. Bloated rulesets significantly complicate auditing processes that require a careful review of each rule and its related business justification.

Some types of problematic firewall rules include:

- Unused rules
- Shadowed rules
- Expired rules
- Unattached objects (rules that refer to non-existent entities, such as users who have left the company)
- Rules that are not ordered optimally (e.g., the rule
- that is "most hit" is near the bottom of the rule list)

These problems drive organizations to take on ad-hoc firewall "cleanup" or "recertification" projects. But, lacking visibility into the entire ruleset over the entire network, as well as the ability to connect firewall rules to their associated business applications, these initiatives frequently bog down resources, without improving security and performance.

Unwieldy and Risky Rules

The Solution

AlgoSec provides rule cleanup across your entire environment. AlgoSec allows you to effortlessly optimize your firewall policy and keep it clean and lean. AlgoSec provides a wide range of actionable recommendations to cleanup, optimize, and tighten the security policy. It can discover and remediate problematic rules, without impacting required traffic flows, reorder rules for optimal performance while retaining policy logic, and automatically trigger change requests.

Its actionable reports identify and help you remove the bloat and clutter from your policy, while AlgoSec's automated change management processes ensure that new rules are optimally designed and implemented so that you don't generate more clutter over time.

Security Policy Consistency Across Multiple Management Consoles

The Challenge

It is difficult to maintain security policy consistency across multi-vendor, multi-topology devices. You may be changing your security policies on some devices, but how can you be certain that your policies are consistent, not conflicting with one another, across your entire network?

Each firewall vendor offers its own unique management console, such as FortiManager, Palo Alto Networks' Panorama, and Juniper Space, to manage all of its devices. Yet, your data center is made up of multiple device vendors, each with their own management console. Cloud vendors also provide their own console that facilitates the day-to-day management of its cloud account. To make network-wide policy changes that span firewalls and clouds, security staff must access multiple consoles forcing enterprises to employ a legion of experts just to implement even a simple change. Changes have to be meticulously coordinated across the many management consoles slowing down progress and introducing the potential for errors.

Security Policy Consistency Across Multiple Management Consoles

The Solution

The AlgoSec Security Management Solution eliminates the need for multiple management consoles, providing vendor-agnostic and multi-vendor change management. By utilizing the AlgoSec Security Management solution, security policies can be consistent across your network. The AlgoSec platform takes a holistic view of your entire network and can identify interconnected rules.

In a single console, users can manage their multi-vendor devices over their entire complex, heterogeneous network topology. There is visibility and automatic change management across the on-premises, public cloud, and private cloud and SDN environment – all within a single management platform. They can even avoid the console altogether.

Users can set their change management workflow to run automatically through the entire application lifecycle - from planning through deployment to production-with zero-touch. Recommended policy changes can also be implemented on their device with ActiveChange. Designed to save time and prevent manual errors, changes are implemented directly on the security control, eliminating the need to manually access and implement each individual change on each management console.

The AlgoSec Security Management Solution also integrates with popular IT Service Management solutions such as ServiceNow, so business application owners can stay within the tools that they are most familiar with in order to manage change requests.

The Cybersecurity Skills Gap

The Challenge

Effective network security professionals are more important than ever. Yet, as network complexity increases, skills specialization also increases. Frequently, there are different teams managing your on-premises network and your cloud networks, with different knowledge about networking and security. Yet, despite the urgent need, there is a severe scarcity in able and certified personnel.

According to a McAfee study, IT leaders need to increase their security staff by 24% to adequately manage the current threat landscape. According to a study by the British government, around 48% of organizations in the UK are unable to carry out basic tasks due to a cybersecurity skills shortage, including setting up firewalls. But these people are simply not available.

The absence of adequately trained security professionals' leaves gaps.

In their report on security deficiencies, ESG found that 33% of responders indicated that their biggest deficiency was cloud security specialists followed by 28% who pointed to a deficiency with network security specialists and 27% who suffer a shortage of security analysts.

Many security positions remain unfilled, putting organizations at risk.

The Solution

Utilizing the AlgoSec Security Management Solution reduces reliance on multiple specialists and, by enabling security policy automation, reduces the stress on your IT team.

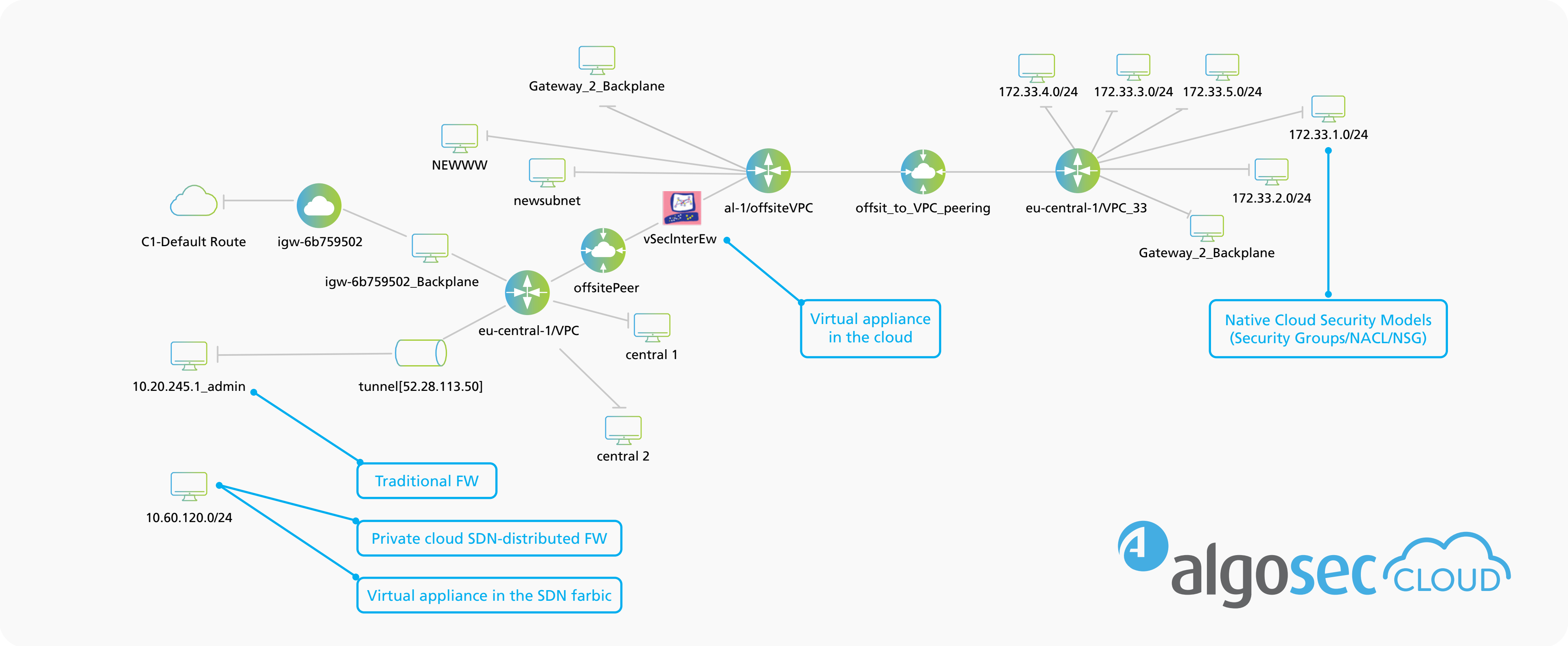
Security policy automation reduces the need to have multiple teams managing your network. It provides visibility over the entire network, and, through intelligent automation, saves time and resources spent doing manual, time-consuming tasks that can be better automated. Leave your security professionals from doing the manual work and let them focus on security strategy.

The AlgoSec Solution

When using the AlgoSec Security Management Solution, users benefit from a hybrid approach, spanning on-premise, SDN and public cloud. This lets them unify security policy management across heterogeneous cloud, software-defined, and on-premise environments.

Users get:

- **Continuous Visibility -** Get a full network map of your entire network estate – both on-premises and in public and private clouds. Ensure visibility of the applications in your network.
- **Application Connectivity -** Quickly and securely provision application connectivity, and avoid network related outages
- **Hybrid Network Change Management Automation -** Leverage a uniform network model and change-management framework that covers the hybrid and multi-cloud environment. Automate firewall change management and eliminate misconfigurations
- **Compliance -** Ensure continuous compliance and drastically reduce firewall audit preparation efforts
- **Risk Management -** Reduce risk through correct security configuration and effective network segmentation.
- **Policy cleanup -** As firewall rules and cloud security groups are constantly adjusted, they can rapidly bloat. This makes it difficult to maintain, increasing potential risk. With advanced rule cleanup capabilities, easily identify unused rules and remove them with confidence.
- **Organizational Alignment -** Align security, networking and application teams, and foster DevSecOps



Virtual appliance in the cloud

Native Cloud Security Models (Security Groups/NACL/NSG)

Traditional FW

Private cloud SDN-distributed FW

Virtual appliance in the SDN farbic

About AlgoSec

AlgoSec enables the world's largest organizations to align business and security strategies and manage their network security based on what matters most - the applications that power their businesses. Through a single pane of glass, the AlgoSec Security Management Solution provides holistic, business-level visibility across the entire network security infrastructure, including business applications and their connectivity flows - in the cloud and across SDN and on-premise networks. With AlgoSec users can auto-discover and migrate application connectivity, proactively analyze risk from the business perspective, tie cyber-attacks to business processes and intelligently automate time-consuming security changes - all with zero-touch, and seamlessly orchestrated across any heterogeneous environment. Over 1,800 leading organizations, including 20 of the Fortune 50, have relied on AlgoSec to drive business agility, security and compliance. AlgoSec has provided the industry's only moneyback guarantee since 2005.