algosec | BUSINESS-DRIVEN SECURITY MANAGEMENT

6 best practices to stay secure in the hybrid cloud

EBOOK

TABLE OF CONTENTS

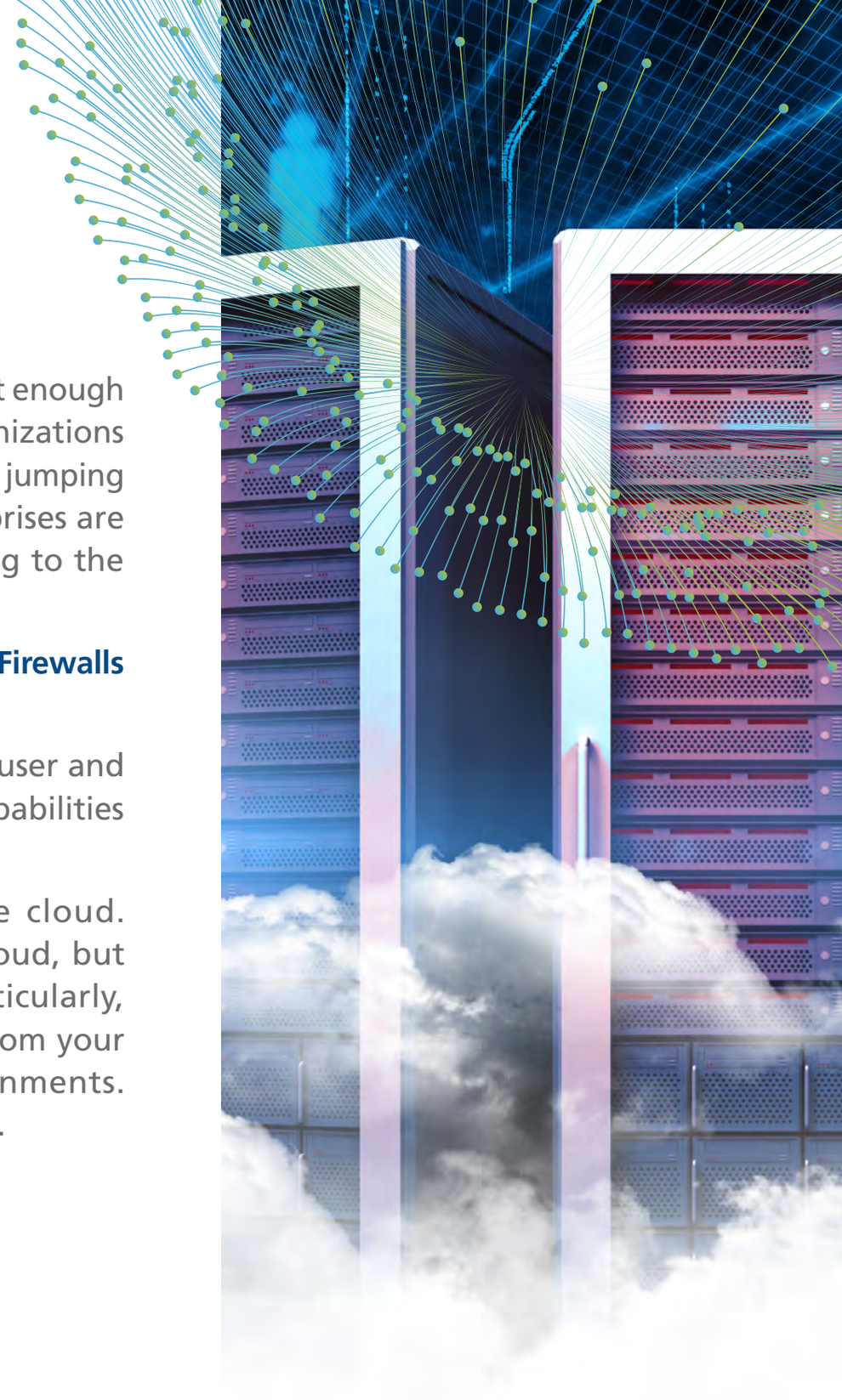
Introduction

Every year we witness more organizations of all sizes investing more in the cloud. A recent report by the Cloud Security Alliance and AlgoSec shows that over half of organizations are running 41% or more of their workload in the public cloud, and 62% of organizations are running multi-cloud environments.

With organizations running workloads in complex hybrid networks – public, private, and on-premises networks – the security landscape is getting even more complex. There are actions you can take, though, to help you dissolve the complexities.

Here are six best practices you should consider to stay secure in the hybrid cloud.

01 Use NGFWs in the cloud



Cloud providers’ native network security controls are not enough to protect your valuable cloud assets and services. Organizations are using the cloud providers’ advanced security controls, jumping from 58% in 2019 to 71% in 2021, and 49% of enterprises are using virtual editions of traditional firewalls according to the Cloud Security Alliance.

But to truly stay secure, you should **use Next-Generation Firewalls (NGFWs) in the cloud.**

Your network needs filtering capabilities. NGFWs are user and application-aware, providing context and important capabilities to manage your network.

Your network is hybrid. Not everything is in the cloud. Of course, you need to control traffic within the cloud, but you also need to control traffic outside it and, particularly, traffic entering and flowing from the Internet and from your on-premises network to your public cloud environments. To do this effectively, you need an NGFW in the cloud.

Using an NGFW will allow you to enjoy advanced Layer 3-Layer 7 capabilities such as:

User awareness and application awareness

Container protection

Threat intelligence

Cloud firewall primer

Cloud firewalls are available from traditional firewall vendors such as Check Point or Palo Alto Networks and, in the form of advanced security controls, from public cloud providers such as Microsoft Azure and Amazon Web Services.

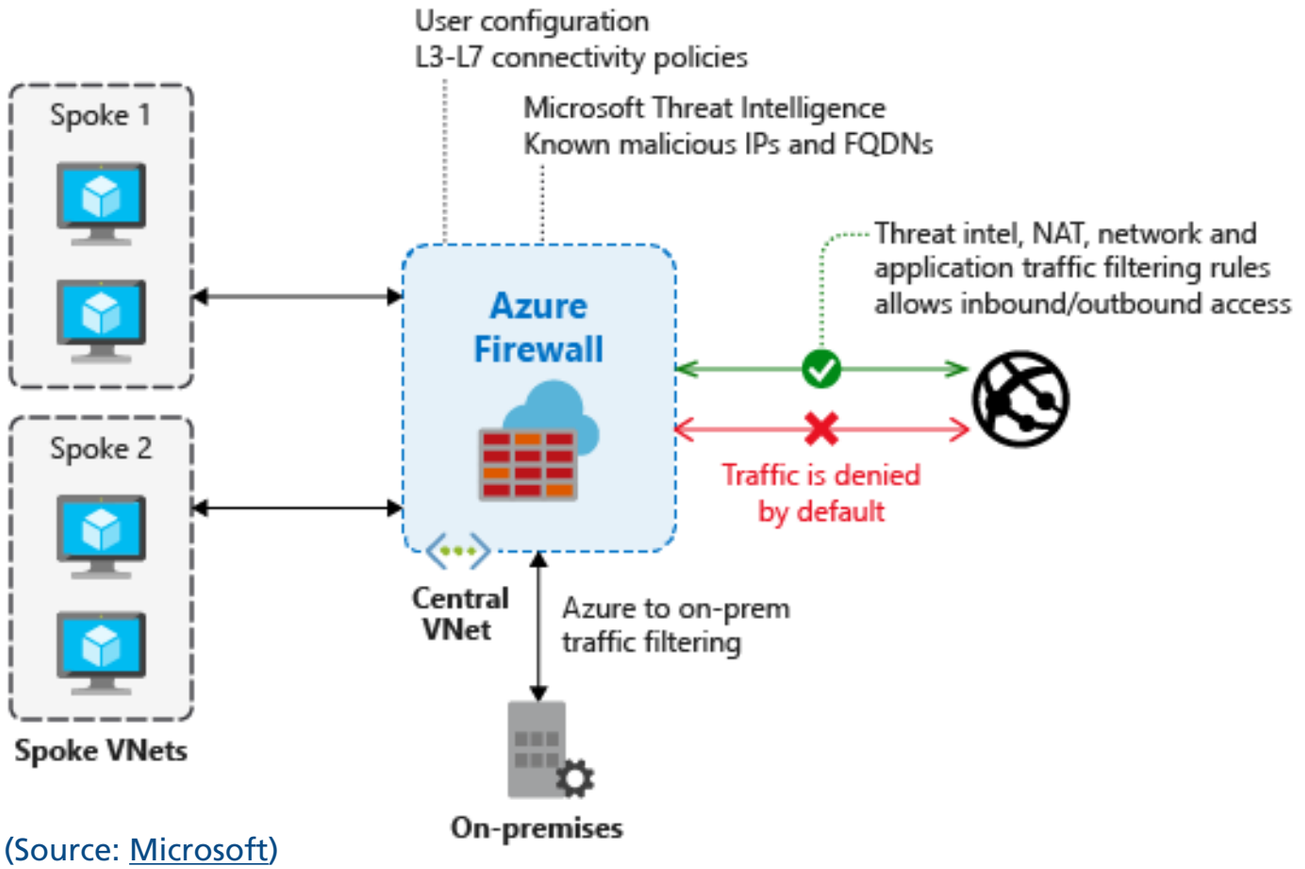
Traditional firewall vendors	Cloud providers & cloud firewall vendors
Check Point CloudGuard	Microsoft Azure Firewall
Palo Alto VM series	AWS Network Firewall
Cisco FTDv	
Juniper vSRX	
Fortinet NGFW	

You should follow the vendor's best practices to choose the ideal deployment method for this security control.

For example, many organizations are using a hub-and-spoke topology where:

- The hub is a VPC/VNET that serves as an entry point for connections coming from a data center or the Internet.
- There’s an NGFW cluster in the hub that serves as a filter in front of all the services hosted in the spoke VPCs/VNETs.

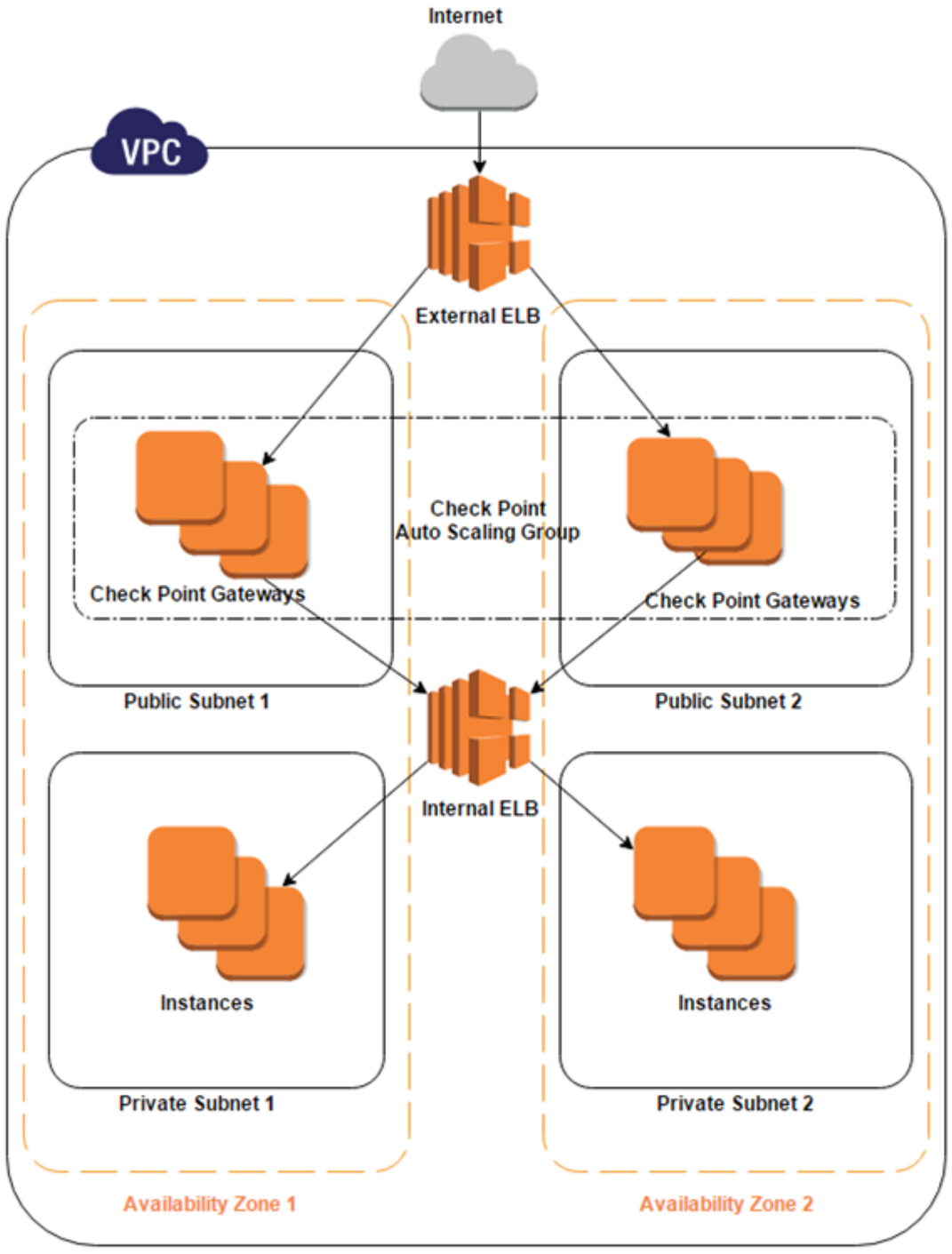
Example (Azure Firewall)



(Source: Microsoft)

In addition, many organizations take advantage of the benefits of auto-scaling clusters to put a proper number of NGFWs that can filter varying traffic volumes. There are many scenarios where this is useful, including properly scaling when there is a seasonal peak of client requests.

Example (Check Point Auto-Scaling group in AWS)



(Source: Check Point)

02 Use dynamic objects

You can’t configure traditional firewalls in the cloud the same way you configure firewalls in an on-premises environment.

On-premises, security policies are typically associated with static subnets or IP addresses. But in the cloud, workloads protected by traditional firewalls don’t use static IP addresses. You need a mechanism that allows you to define a policy that protects this dynamic nature of cloud workloads.

Use dynamic objects in your NGFWs that communicate with and inside the cloud.
This helps you refrain from frequent configuration changes and keep you from introducing additional risk into your network.

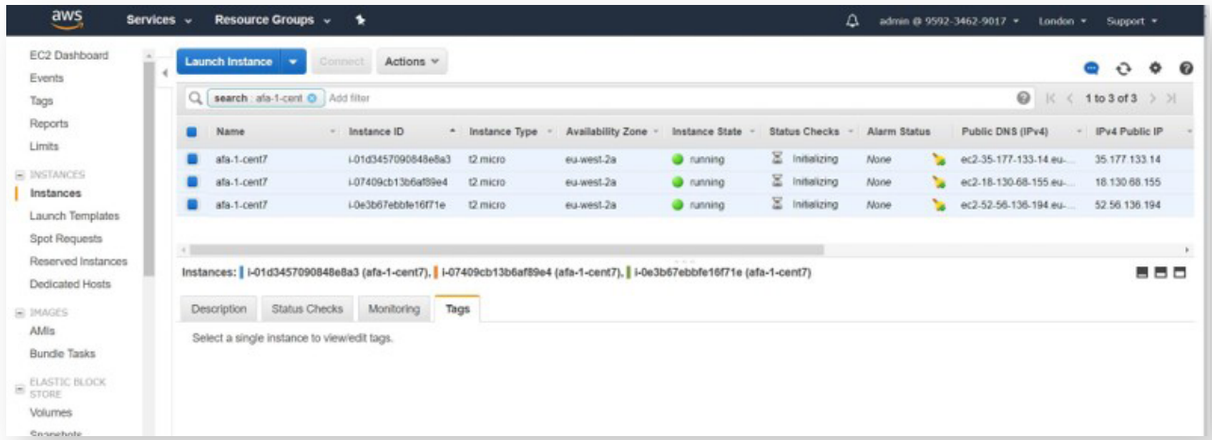
NGFW dynamic objects allow you to match a group of workloads (e.g., instances, VMs, Kubernetes clusters) using cloud-native categories such as tags, all instances protected by a certain security group, and more. For example, you might have AWS EC2 instances or Azure virtual machines with a tag such as “Application=Payroll.” When you configure a dynamic object on the NGFW matching this tag, you can use the object in a rule’s source or destination to allow only certain traffic to this application. This policy will be properly enforced even though the instances IP addresses may change.

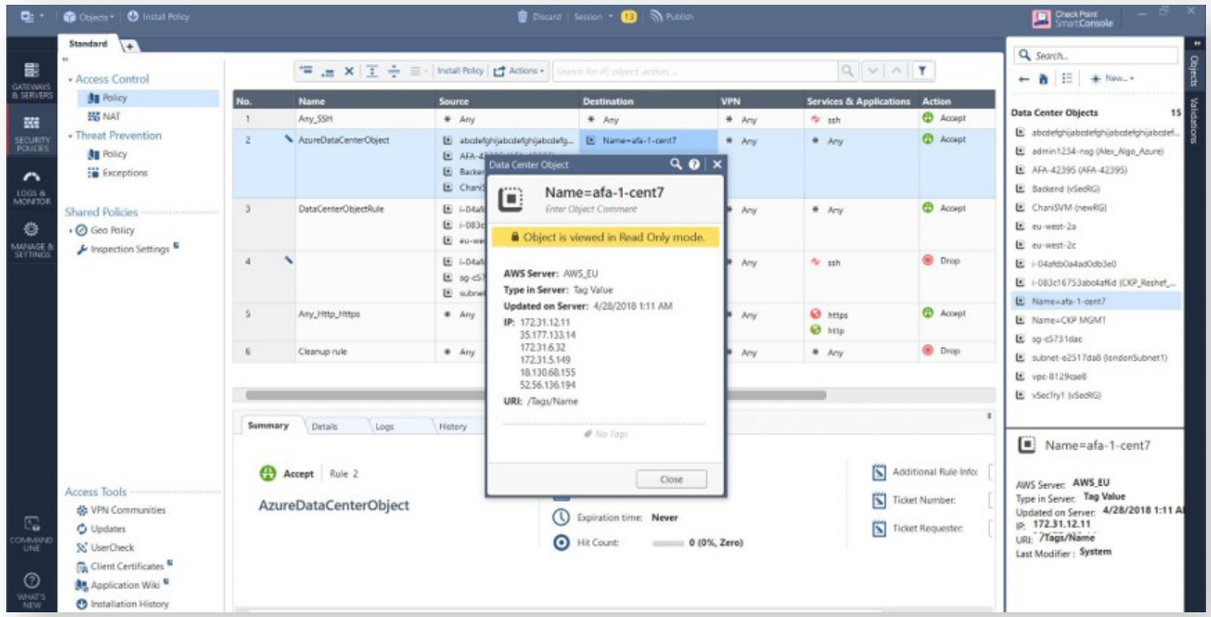
Examples of dynamic objects:

Palo Alto dynamic address groups

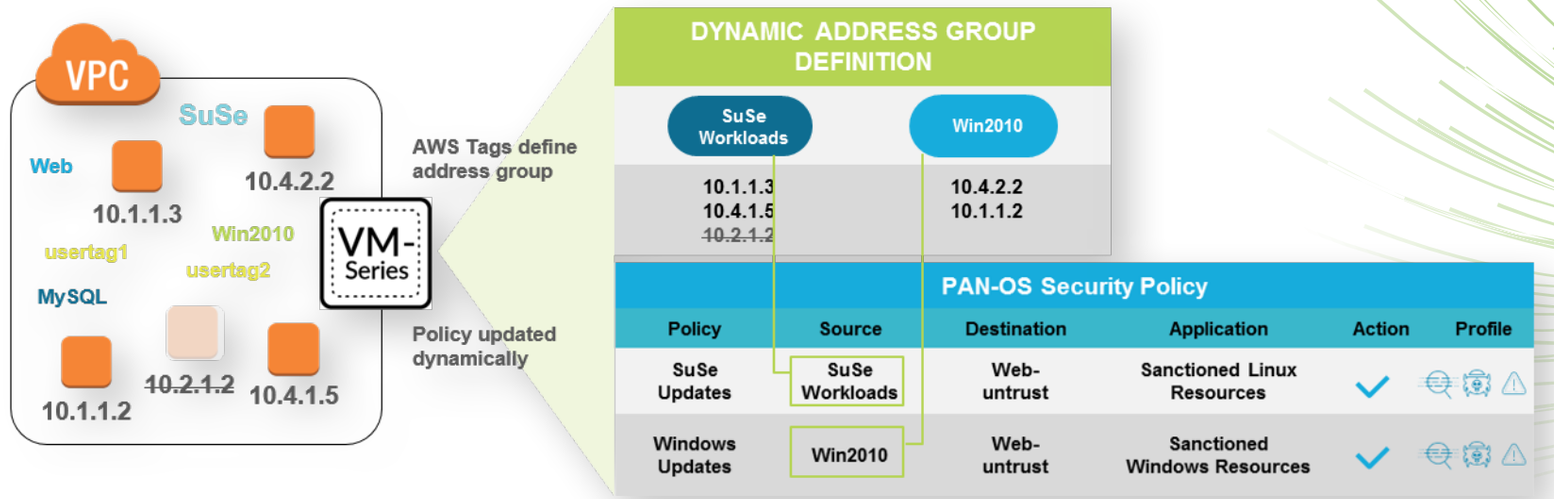
Check Point data center objects

Fortinet Fabric connector objects





In this diagram, we can see a simple yet powerful and dynamic Palo Alto NGFW policy consisting of two rules. This policy allows traffic for operating system (OS) updates where the source in each rule is a dynamic object that holds the IPs of the matching AWS instances based on the OS criteria. The relevant instances continue to be protected even if the IP changes.



03 Gain visibility over your entire hybrid network

You can’t protect what you can’t see.
Visibility over your ENTIRE hybrid network traffic is crucial.

Some challenges of visibility into the cloud include:

Multiple cloud vendors and security controls within the cloud environment.

Cloud infrastructure is not owned by the security team.

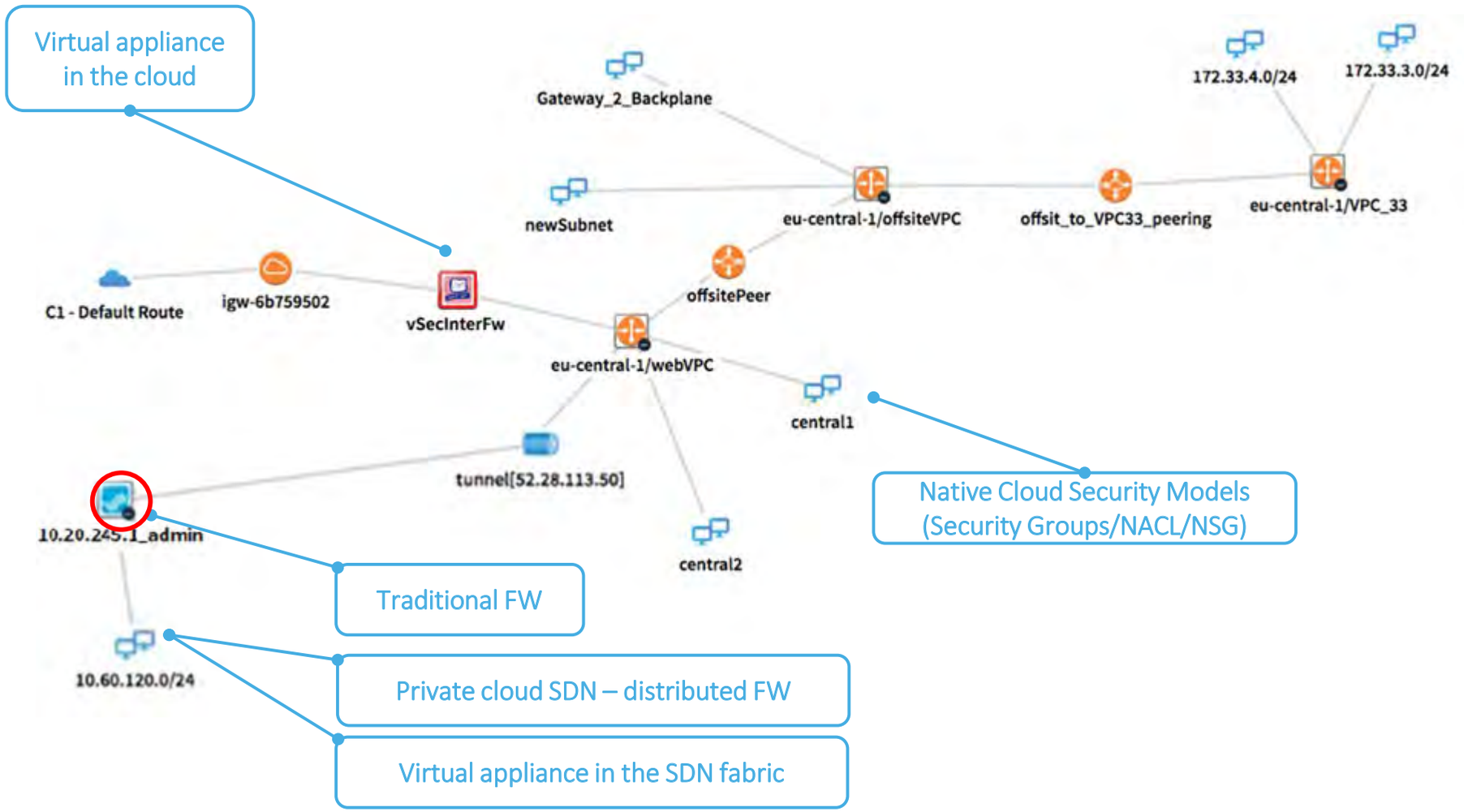
Difficult to understand network structures and flow paths.

Hard to track the operations, assets and security controls.

Think about security throughout your entire network, not only in the cloud. Consider the client subnets on-premises and on the internet that consume those services and how they communicate with each other.

By using the AlgoSec solution, you can **gain full visibility of network topology and traffic in your entire hybrid network.** Extend visibility and analysis from the cloud to your entire hybrid network, no matter where your traffic resides – public and private cloud or on-premises. Get a holistic view of your network traffic.

Get instant visibility of your cloud assets and security controls. Pinpoint and troubleshoot network connectivity issues resulting from security policies.



04 Evaluate and remediate risk on the entire hybrid network path and not just within the cloud

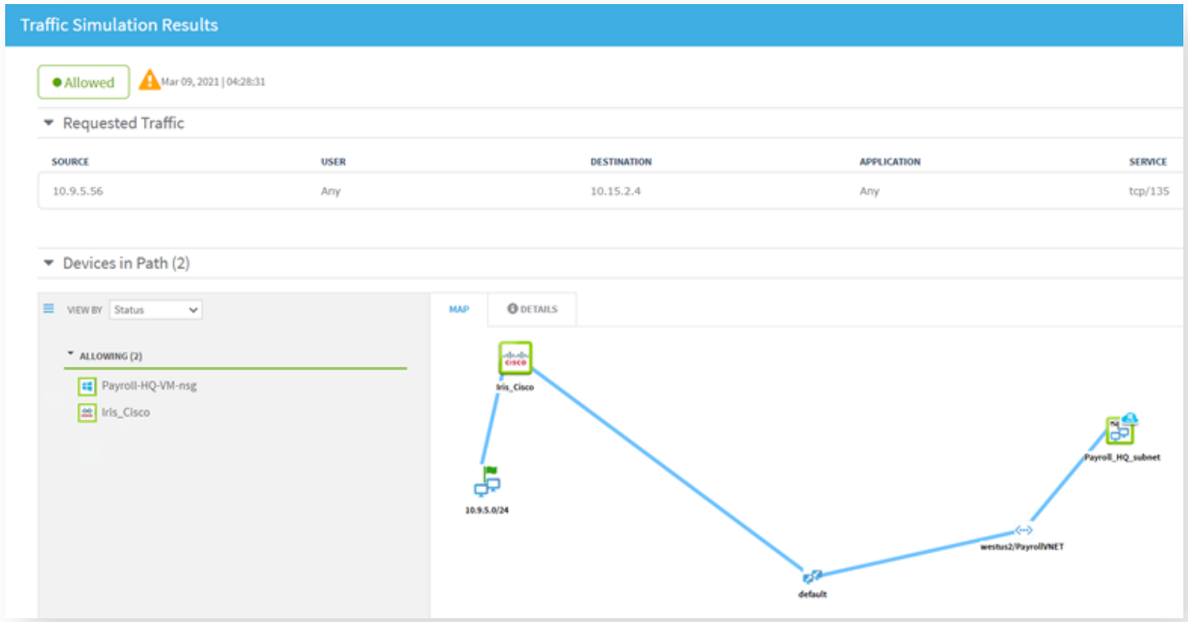
Keeping up with risk and compliance is a challenge and requires:

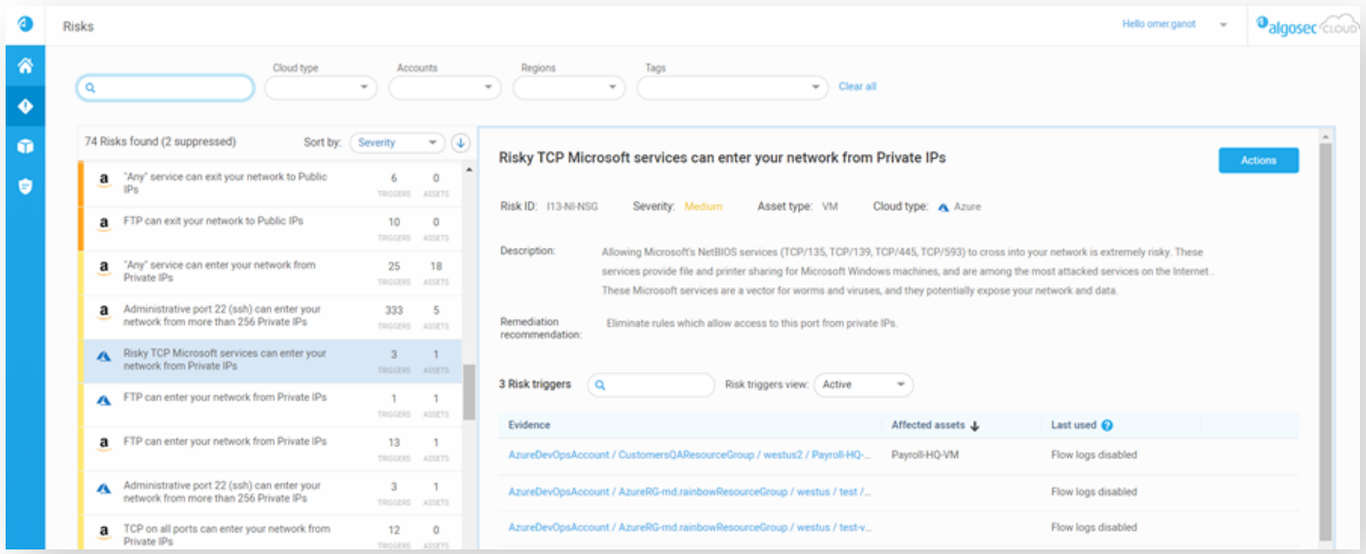
- Identifying risk across the entire hybrid network – all using different security controls.
- Risk remediation across the different controls.
- Keeping up with constantly changing internal and regulatory standards.
- Maintaining ongoing documentation and audit trails.
- Obtaining the compliance status of the entire network.
- Preparing for audits.

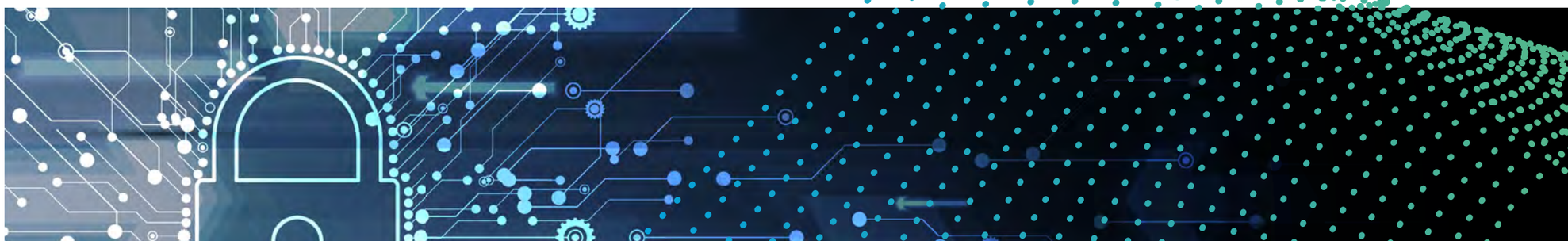
While most public cloud providers have risk assessment capabilities for their native security, they lack risk analysis and remediation for other cloud vendors.
As cloud configuration is complex, it’s hard to identify misconfigurations in real-time. Manual changes made even with the best of intentions introduce risk.

And, of course, your network traffic isn’t just in the cloud, but it also transverses throughout your entire hybrid network. You need to identify and remediate risky network traffic throughout the entire path.
It’s important to see and evaluate ALL the traffic on your network.

By using the AlgoSec solution, the analysis and remediation of your network’s risk aren’t siloed. **Analyze the traffic and identify risk over your entire hybrid network, no matter where your traffic resides.** Risky security policies, their affected assets and rule usage are identified, and instructions are provided to fix the risky policies.







05 Clean up cloud policies regularly to make sure they are maintainable and risk-free

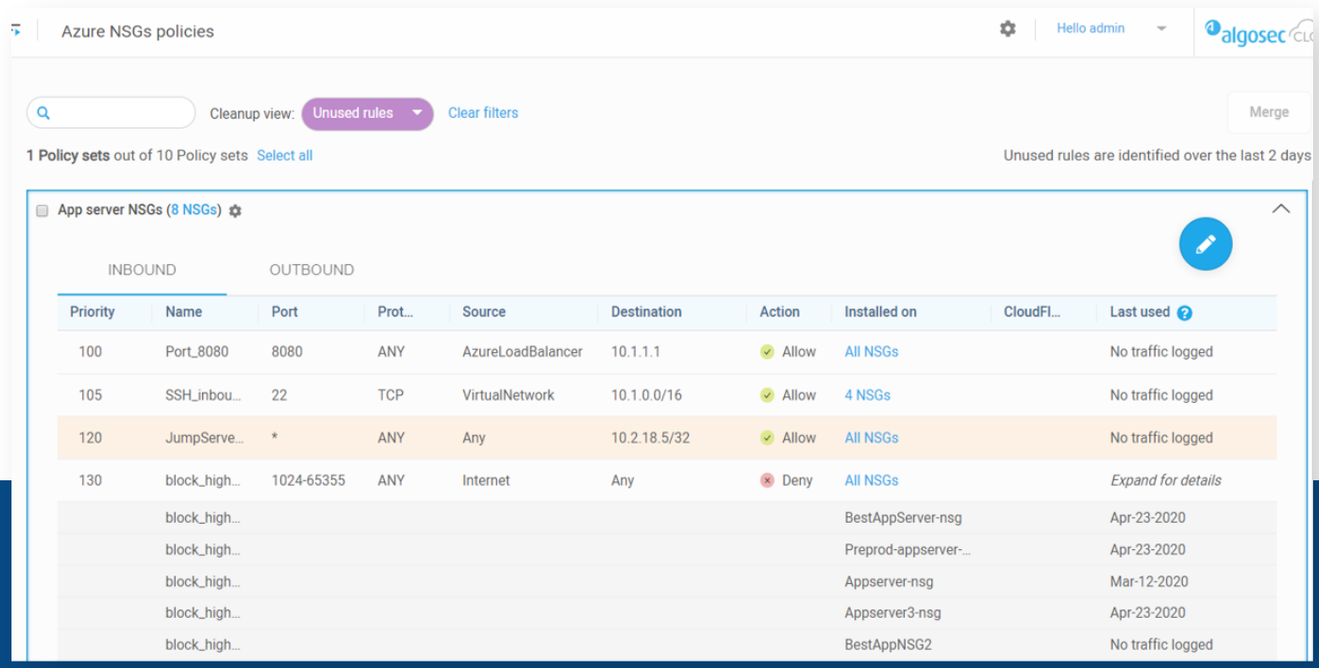
IT and cloud operation teams are often moving fast and… break security.

As cloud security groups are constantly adjusted, they can rapidly bloat. This makes it difficult to maintain.

Even after you identify unused security rules that you want to remove, cleanup may be cumbersome and time-consuming. But, if you don’t do it, it will be even worse as time goes by. Adding more and more rules will lead to you hitting a wall and the security rule limit. You won’t be able to add more rules and may end up indiscriminately deleting crucial rules. And, of course, you are also adding more risk to your network, leaving big security holes.

You need to create a method and process to **clean up cloud security policies quickly and efficiently without introducing application outages.**

Using the AlgoSec solution, you can easily identify and remove unused rules. Proactively detect misconfigurations to protect cloud assets, including cloud instances, databases, and serverless functions. Easily identify risky security policy rules, the assets they expose, and whether they are in use. Unused rules can more easily be removed. This ensures that rule cleanup is accurate, avoids application outages and is efficient.



06 Put “Sec” into DevOps: Perform a risk check as part of the cloud change pipeline

Your cloud security groups are typically managed by the cloud team or DevOps and not by SecOps. The core of DevOps is to run fast and enable agility.

But what about security?
DevOps and application developers are focused on delivering new and innovative products. Security isn’t necessarily the priority. They leave traffic open too wide because they don’t want to stop at each step and wait for approval from the security team, delaying delivery.

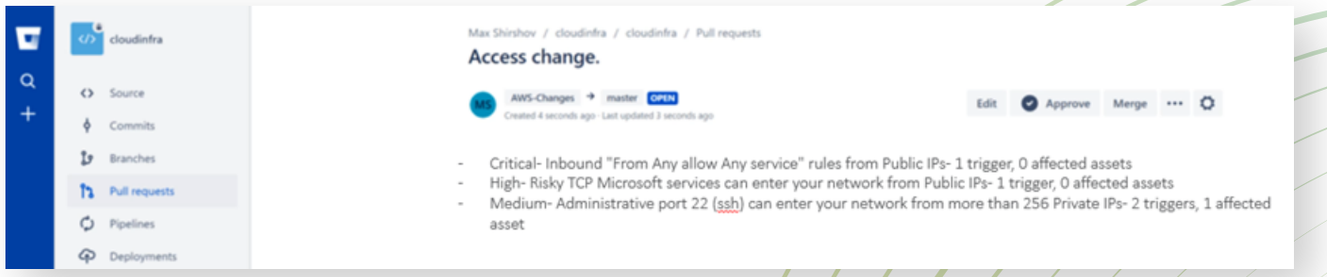
Security should be a proactive part of the DevOps process. Use relevant tools to **make risk-check part of the cloud security group’s change pipeline.** The what-if risk check will make sure the rule is not too wide and minimize misconfigurations. This way, security simply becomes another delivery requirement.

Run what-if risk check for cloud security group changes as part of the code pull request. Tighten the changes to eliminate risks. Once the risk is taken care of, then push to production.

This is a win-win situation. It prevents network security from becoming a bottleneck to delivery, while ensuring that the DevOps team is accountable for the security of their applications, without interrupting their workflows or making them learn new tools or take on new responsibilities.

Shift left. Find risk before release, not after the fact. Ultimately, this accelerates delivery and enables agility, so you are not slowed down by a security failure.

Security at the speed of business.
How can you say no?



Conclusion

Your hybrid cloud security is a core part of your network security.

It doesn't mean it has to be complex. With these six best practices, you can make hybrid cloud security management... Manageable.