

Case Study: Optimizing Network Security and Accelerating Operations for a Major Telecommunications Provider

Industry: Telecommunications

Challenge

A large, international telecommunications provider grappled with the immense complexity of managing network security across its sprawling, hybrid infrastructure. This encompassed traditional on-premise data centers, extensive legacy systems, and rapidly expanding cloud deployments in environments like AWS and Azure. Their reliance on manual methods for firewall, **security group**, and network policy management was incredibly slow, frequently resulted in configuration errors, and created significant operational bottlenecks. This lack of centralized visibility made it nearly impossible to identify and mitigate security risks in real-time, impacting service resilience and the overall integrity of their network and customer experience.

Solution

The telecommunications provider implemented AlgoSec Cloud Enterprise (ACE) as a central platform to automate and unify the management of its cloud network security policies across this incredibly diverse environment. ACE provided unprecedented centralized cloud network visibility, offering the security team a unified view to manage and control security rules across all their cloud platforms (AWS, Azure), including the configuration and enforcement of **security groups**, and a multitude of firewall vendors. The platform normalized complex policy structures, simplifying configurations and ensuring consistent application of security across their global operations. Furthermore, ACE offered application-centric visibility, automatically discovering critical application connectivity and dependencies across their entire network. This provided a crystal-clear understanding of potential security risks to core telecom services, ranging from voice and data to their emerging 5G infrastructure. Automated change management workflows dramatically accelerated the deployment of security updates and new network features, all while ensuring accuracy and minimizing downtime.

Key Benefits & Results

By leveraging ACE, the telecommunications provider achieved substantial improvements in its security posture, operational efficiency, and ability to deliver new services faster:



Enhanced Operational Efficiency & Speed

- **Accelerated deployment of new telecom services and network features (estimated 30-40% faster):** By automating security policy management, including **security group** configuration, and integrating it into their deployment pipelines, the company could roll out new offerings much more quickly and reliably.
- **Reduced time spent on firewall rule and security group management by over 60% (estimated):** Automating tedious manual tasks freed up valuable security personnel to focus on more strategic initiatives.



Strengthened Security Posture & Risk Mitigation

- **Centralized network visibility:** ACE provided a "single pane of glass" for viewing and managing security policies, including security groups, across their entire hybrid network, significantly simplifying oversight.
- **Reduced network misconfigurations by a significant margin (estimated 70%+):** Automated checks and policy enforcement, encompassing firewall rules and security groups, led to far fewer errors, drastically strengthening the security of their vast and complex network.
- **Application-centric visibility for critical services:** The ability to discover and visualize application flows helped the provider understand and secure the specific risk exposure of their core telecom services and underlying infrastructure, with a clear understanding of how security groups contributed to overall application security.

Conclusion

By implementing an automated and intelligent security policy management platform, this major telecommunications provider successfully tackled the complexities of securing its vast and evolving hybrid network. The centralized, automated, and application-aware approach not only bolstered their security posture against emerging threats by effectively managing firewalls and **security groups** but also dramatically improved operational efficiency, enabling them to deliver new services faster and ensure consistent network resilience for their millions of customers.