tufin
The Security Policy Company.

Network Security Without Borders

Unifying Hybrid Security Policy Management Across Clouds and On-Premise

4 Best Practices for Hybrid Security Policy Management

Executive Summary

As enterprises expand their ecosystems across on-premises and multi-cloud environments, network security policy management grows more complex. Hybrid infrastructures enable unprecedented flexibility, but they introduce new challenges. Organizations struggle to maintain consistent, secure, and compliant policies across diverse platforms, technologies, and vendors. Simultaneously, security and network teams increasingly need robust security policy management practices that respond to their networks' diverse deployments, vendors and technologies. In response, many companies seek solutions that ensure seamless security, reduce operational overhead, and help meet compliance standards.

This white paper outlines challenges most companies experience and suggests the following four best practices for managing hybrid policies:

- Implementing unified policy frameworks to create consistency
- Using automation to reduce manual tasks
- Continuously monitoring compliance to reduce risk
- Consolidating network security policy management to enable collaboration

By empowering network, security, and IT teams, organizations can maintain a cohesive security posture across both cloud and on-prem environments. By implementing these strategies, enterprises can gain better visibility, streamline processes, and improve security across their entire infrastructure—ultimately reducing risk, optimizing operations, and streamlining compliance.

Challenges of Managing Hybrid Environments

Navigating hybrid environments presents several challenges, but the single largest challenge lies in the diversity and complexity of these environments. Organizations must address these challenges strategically to manage the delicate balance between cybersecurity risk mitigation and business operational uptime.

Visibility Gaps

A primary challenge for most organizations is that they lack comprehensive visibility across their complex networks. In a modern enterprise network, IT and security teams struggle with managing various network connections, including:

- Countless endpoints, including databases, on-premises data centers, user devices, Internet of Things (IoT) devices, and cloud services
- Remote users, including people working from home, working while traveling, or third-party contractors
- Software-as-a-Service (SaaS) applications with different connectivity requirements

All of these can lead to blind spots in your network security - putting your organization at risk.

Inconsistent Policy Enforcement

As organizations grow, different departments and teams might implement their own policies tailored to specific needs. This policy fragmentation can result in an intricate and often inconsistent security posture.

In hybrid environments, organizations may deploy multiple firewall vendors for various reasons, including:

- **Zero-day vulnerabilities:** defense-in-depth as part of third-party risk management (TPRM) processes
- **Service availability:** vendor service disruption unable to create a single point of failure
- **Legacy and NGFW:** collection of network security and management tools over time, including cloud, SASE, SSE, SD-WAN, and Edge devices
- **Vendor capabilities:** vendor purchase based on best technology for desired use case

In a multi-vendor ecosystem, organizations often struggle with:

- Implementing and applying consistent firewall rules and network configurations
- Proactively identifying security policy violations
- Effectively applying fixes or exemptions in a timely manner

This lack of cohesion can lead to compliance risks, as auditing and reporting become more complex across platforms.

Manual Management

One of the most pressing challenges in this landscape is the reliance on manual processes for policy management. In hybrid environments, manually configuring, updating, and auditing security policies across multiple platforms is time-consuming and prone to error.

Many network and security teams still rely on reactive, time-consuming processes, like:

- Using spreadsheets for tracking security policy changes
- Unstructured change management processes that increase misconfiguration risks
- Remediation processes riddled with human error risks
- Time-consuming audit and compliance practices that increase costs
- Limitations on network operations and security teams who lack visibility into network architecture

These practices lead to operational challenges that increase administrative costs and impact network performance, including:

- Inability to identify who made changes or why they made them
- Fear of modifying rules that increases the overall number
- Rule bloat that introduces latency
- Audit preparation fatigue from reporting tasks and document collection

At the end of the day, manual processes increase an organization's data breach risks. Without visibility into change management, the organization lacks insights into critical security elements like:

- Increased misconfigurations
- Vulnerabilities that attackers can exploit
- Compliance violations that can lead to fines or penalties
- Costly delays when implementing changes

This burden on IT and security teams often prevents them from focusing on more strategic initiatives, as they are stuck in reactive mode, responding to policy issues one by one.

Compliance Risks

As the regulatory landscape continues to change, organizations struggle to align their security controls to compliance mandates. Many organizations need to comply with multiple regulatory and industry-specific requirements, including:

- PCI-DSS for managing payment card data
- NIST Cybersecurity Framework for implementing a risk-based analysis that defines controls
- ISO 27000-series for managing an information security management system (ISMS)
- HIPAA for security and privacy of electronic protected health information (ePHI)
- SOX for proving internal controls over financial reporting

Organizations use one compliance framework, like NIST, as the basis for mapping their controls to other requirements, like HIPAA or PCI-DSS. However, without visibility into where covered data resides and the networks that transmit it, they increase compliance violation risks, making them more likely to face fines.

Security Silos

Managing on-premises and cloud networking environments separately creates security silos and fragments security strategies. When the organization has traditional firewalls co-existing with cloud infrastructure, network, security, and IT teams struggle to gain insights across public cloud, firewall, and application configurations.

Managing security in different vendor-supplied portals leads to issues like:

- Gaps created by disconnected public cloud and firewall policy configurations
- Proliferation of unused and redundant rules across infrastructures
- Inability to assign responsibility for managing services and application security policies
- Incomplete information about securing applications

Managing these rulesets separately can lead to improperly defined rules that create security gaps that threat actors can exploit, essentially expanding the organization's attack surface.

4 Best Practices for Hybrid Policy Management

No one-size-fits-all approach exists to managing security, since every organization has a different risk tolerance and network architecture. However, by adopting some best practices for security policy management in hybrid environments, organizations can maintain robust security and improve network performance.

Unified Policy Visibility

By implementing solutions that offer unified policy visibility, IT, network, and security teams gain a single, consolidated view of firewall rules and application firewall policies deployed across on-premises and cloud environments.

Using a central hub of security truth enables everyone involved in network and security management to understand the network architecture and data flows. With a comprehensive visibility into network topology, organizations achieve benefits that include:

- Expedited troubleshooting, improving incident response times and alert-to-fix timelines
- Consistent documentation of and control over firewall rules and configurations
- Network change tracking that reduces audit preparation fatigue

Automation and Orchestration of Policy Changes

By automating or orchestrating change management processes and their documentation, organizations can build risk management, compliance, and security into daily network management responsibilities.

With automation and orchestration, organizations achieve benefits like:

- **Reduced error risk:** defined workflows that identify potential security risks and enforce defined processes
- **Faster policy changes:** approval workflows that ensure change review and approval to reduce time spent on change tracking and follow up activities
- **Improved consistency access platforms:** automated compliance checks and reporting to monitor firewall configurations against regulatory standards and internal security policies before implementing changes

Centralized Compliance Management

Centralized network visibility and automated network security policy management enable organizations to implement continuous cross-network compliance. With centrally defined policies mapped to compliance requirements, organizations can meet and maintain compliance across disparate network tools, including firewalls, NGFW, routers, switches, SASE, SD-WAN, and SDN.

By centralizing hybrid network policy management, organization can improve regulatory compliance processes by:

- Implementing and continuously enforcing the principle of least privilege across all network segments
- Automating documentation collection and reporting to reduce audit costs
- Proactively analyzing risks within automated change workflows
- Reducing complexity by identifying and decommissioning unnecessary rules
- Improving incident response by enriching processes with accurate network data

Collaboration Across Teams

For a digitally transformed business, network security policies no longer operate in a vacuum. They are part of the organization's overall IT, security, and application management strategies.

Despite having a single location for managing and monitoring network security policies, organizations should consider integrating the data the platform generates across other enabling technologies:

- **ITSM:** Enhancing existing change management process, automatically populating network change tickets
- **IPAM:** Maintaining network segments by automatically synching with a network for a single source of truth
- **Vulnerability-based Change Automation:** Enabling risk-based access request workflows to reflect the results of vulnerability scan results

The Role of Automation in Policy Management

As organizations scale their operations, the complexity of their network security policies increases. This demands a more efficient and reliable method of policy management than traditional manual processes. Automated tools can handle large volumes of data and numerous policy changes, ensuring that security policies remain robust against cyber threats and adaptable to evolving network requirements.

Reduction in Human Errors

Manual configuration of security rules can lead to misconfigurations that expose networks to potential threats. Automation and orchestration tools ensure that firewall policies and other security policies are implemented correctly by following predefined templates and protocols.

With well-defined workflows, organizations can maintain consistency across traditionally manual processes like:

- **Risk analysis:** Embedding risk analysis into workflows reduces the subjectivity of manual processes to ensure consistency with internal controls and risk tolerance
- **Managing responsibility:** Defining responsible parties within the workflows ensures that the appropriate people will review changes prior to implementation
- **Network segmentation and microsegmentation:** Automating consistent policies builds network segments based on how people use networks to improve productivity while still limiting access appropriately

Faster Policy Updates

In dynamic IT environments, the ability to swiftly propagate policy changes across network perimeters is crucial. Automated systems can update security rules across both on-prem and cloud infrastructure in real-time, reducing potential exposure windows to external threats.

WIth automated policy changes, organizations minimize overall remediation efforts, enabling them to gain benefits like:

- **Enhanced productivity:** Automated network changes empower network security teams to implement changes and swiftly accelerate incident response times.
- **Improved metrics:** Consistent, faster changes across on-premises, cloud, and edge infrastructure improves access changes SLAs from days to minutes
- **Faster time-to-value:** Simplifying consistent management enables faster, safer workload connectivity and application delivery

Continuous Compliance

Automated solutions offer real-time monitoring to detect compliance violations instantly. They can correct issues before they escalate, ensuring that organizations adhere to regulatory compliance requirements consistently. This capability is especially vital in hybrid cloud environments, where maintaining compliance across multiple platforms can be challenging without centralized management and automation.

Organizations can leverage continuous compliance solutions to manage activities and controls across multiple regulations, mandates, and frameworks by:

- Leveraging ready-made templates to rapidly configure policies so they align with industry regulations and standards
- Automating policy non-compliance alerts, remediation efforts, and change processes
- Generating automated audit trails for customizable audit reports
- Promptly responding to non-compliance issues while automating the documentation that proves compliance

Tufin: Consistent Hybrid Policy Management for Enhanced Security, Operations, and Compliance

As zero trust network architectures become a security and compliance best practice, you need solutions that enable you to achieve these objectives. Tufin centralizes control and management of your on-premises and multi-cloud environments, Providing you the visibility necessary to implement and enforce least-privilege access consistently without compromising business agility.

Tufin enables you to centrally manage network security policies across all assets, cloud resources, and perimeter defenses with vendor-agnostic Unified Security Policies (USPs) for control and consistency across disparate technologies, vendors, and environments. Further, network and cloud security teams can collaborate more efficiently, enabling them to centralize and automate security policy design and deployment to protect cloud-native services and on-premises devices and data.

With the ability to automate processes and standardize policies, you can meet compliance documentation generation, collection, and reporting requirements. Tufin's pre-defined regulatory compliance templates enable you to easily define segmentation policies in alignment with mandates and frameworks your business needs. With proper segmentation and security zone management across heterogeneous devices, you always know where critical assets reside for improved protection and security management.

Tufin's network topology maps visualize all network traffic so you have real-time application and service-level visibility and control across all cloud assets, applications, services, and traffic. By having continuous insights across hybrid networks and infrastructure, you can automate time-consuming, error-prone manual tasks and build risk-aware workflows that enforce policies and alert you to potential network security issues. These risk-based automations enable you to achieve up to a 90% reduction in network change SLAs for faster time-to-value on application deployments.

To see how Tufin can help you manage security policies across a hybrid environment, contact us for a demo today.