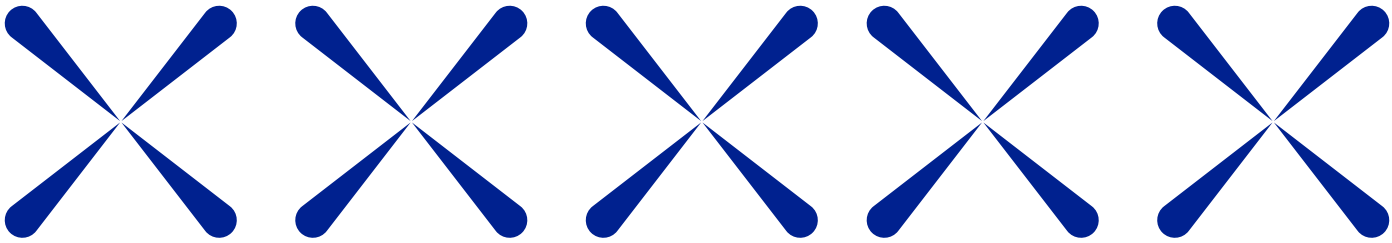
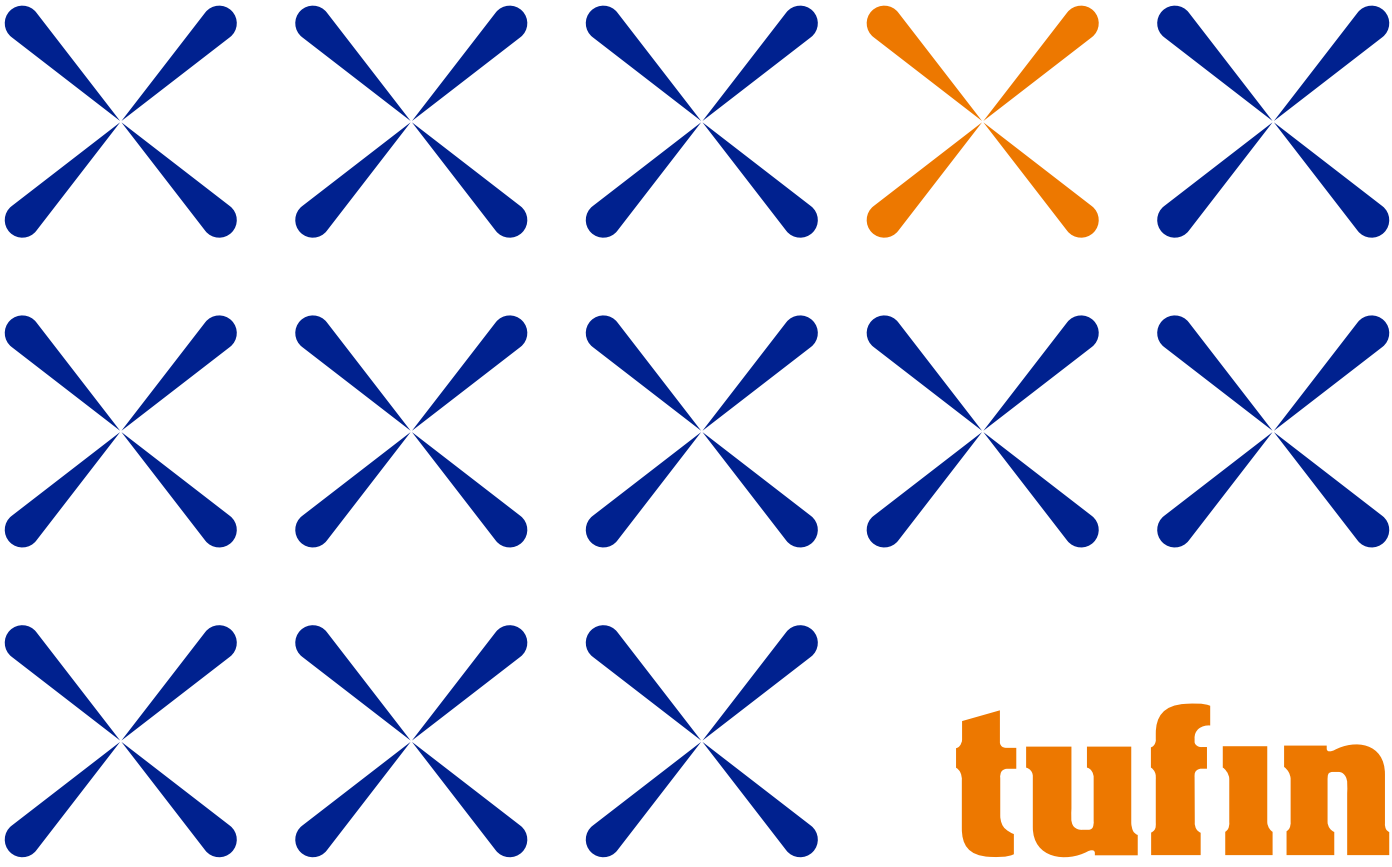


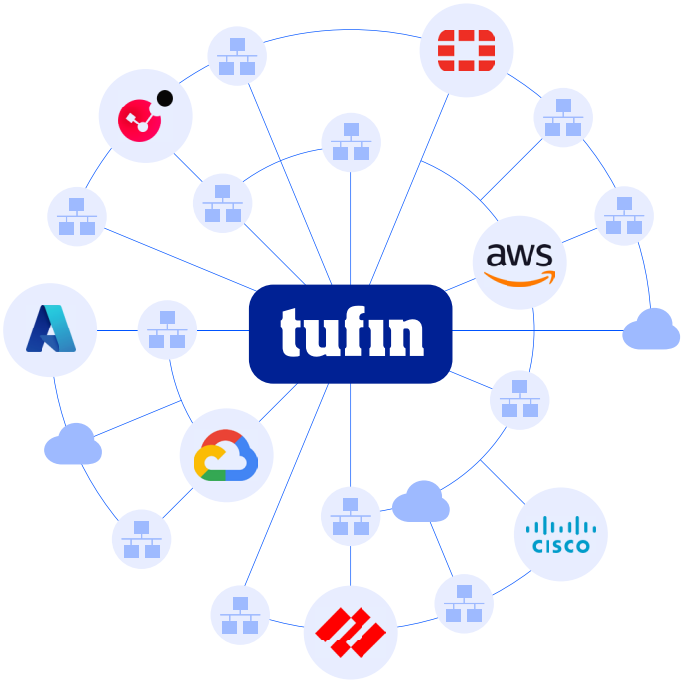
Future-Proofing Network Security: A Maturity Model for Protecting Hybrid Clouds Today



tufin

Network operations and security teams struggle to manage growing, complex network environments. As organizations add more applications that support business objectives, these teams need to secure connectivity, reduce exposure, and maintain availability. Simultaneously, the teams responsible for designing and implementing changes often use time-consuming, error-prone, manual processes and spreadsheets.

Without streamlined security policy management and network change processes, change design and implementation can create delays, increase costs, and slow down time-to-market.



The modern hybrid network infrastructure spans across:

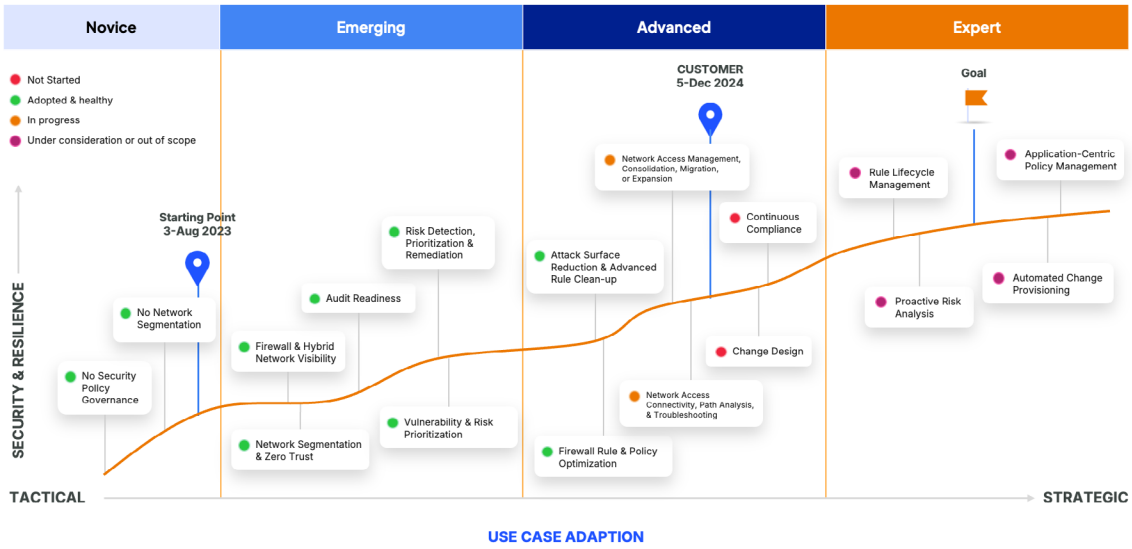
- On-premises data centers
- Public and private clouds
- Distributed edge environments
- Remote employee access from nearly everywhere

Making this even more complex, this diverse infrastructure is secured and connected using various technologies, including but not limited to:

- Legacy firewalls
- Next-generation firewalls (NGFW)
- Cloud-native security controls
- SASE
- SD-WAN

As a result, network security teams face significant challenges in managing this complex, multi-technology ecosystem. The sheer variety and distribution of security tools creates a substantial burden, making it difficult for teams to implement consistent, efficient, and predictable security policies across the entire infrastructure.

Operationalizing network security policy management.



Businesses and organizations struggle with managing their on-premise and cloud network security policies across their firewall estates, SASE deployments, and other technologies in a consistent, predictable and efficient manner.

Network operations and security teams recognize their struggles, but they often face challenges articulating the issues they face. Further, as with every other security and compliance issue, every organization is different.

To make an informed decision on how to mature their network security programs, organizations should think about their current state of network security policy management processes. As part of these considerations, you may want to think about options like:

- Weighing the positives and negatives for potential projects
- Time spent managing the high volumes of rule change requests
- Purchasing technologies to streamline manual processes

The company just beginning to scale its network environment will have different needs from the company leveraging some—or even a lot of—automation and orchestration.

With a network security policy management maturity model, decision-makers can identify:

- ✓ Current network security capabilities
- ✓ Challenges to overcome
- ✓ Specific opportunities to improve
- ✓ Current risks to their network security posture
- ✓ Technologies and functionalities necessary for maturing their network security and compliance posture

In this white paper, we will dive into a network security policy management maturity model allowing you to self-score how mature your network security program might be, what one thing you can do next to improve it, and how you might be able to map out a long-term strategy to continuously improve your capabilities and your team's success.

What Is the Network Security Policy Management Maturity Model?

Network security policy management is an ongoing process and a program that requires continuous care and feeding. Every organization begins at a different point in the journey. The network security policy management maturity model offers a crawl, walk, run approach for organizations to define their current state and set performance metrics for improving processes.

As you seek to improve network security while scaling digital operations, a maturity model enables network operations and security teams to gain insight into how current technologies and processes hinder objectives. To optimize performance and security, organizations should make informed decisions about technologies and processes.

When beginning the network security journey, you should first identify which of the following maturity levels best define its current state:

01 **NOVICE**

Risky, error prone processes, characterized by no security policy governance and a lack of network segmentation.

02 **EMERGING**

Simplified processes with network visibility and insights, characterized by visibility, network segmentation, security policy governance, risk detection, risk and vulnerability prioritization, access control optimization audit readiness, and initial attack surface reduction.

03 **ADVANCED**

Predictable automated network policy and risk management processes, characterized by firewall optimization, attack surface reduction, network access management processes, change design, and continuous compliance.

04 **EXPERT**

Risk-informed, end-to-end automated network security change processes characterized by proactive risk analysis, rule life cycle management, automated change provisioning, and application-centric policy management.

01 The Novice
Identifying the Need for Growth and Improvement

At the Novice level, an organization recognizes that the scale of its network environment is becoming more than the current team can manage manually. The network operations and security teams engage in responsive, ad hoc activities rather than proactive processes, creating a sense of urgency and necessity characterized by:

- Unstructured processes for network and policy changes
- Likelihood of mistakes and difficulties correcting issues
- Growing attack surface
- Weak network security posture
- High potential for lateral threat actor movement
- Makes everything time consuming, costly, and risky

The current lack of tooling increases network security and performance risks as the teams struggle with:

- Excel-based security policy management
- Unstructured network & policy change management
- Human error-prone processes with difficult remediation
- Operations due to limited or no network visibility
- Manual compliance and audit practices

With a network lacking segmentation and no security policy governance, the organization faces operational challenges like:

- Lack of visibility into who made changes or why they made changes
- Fear of modifying rules that increases the number of rules
- Rule bloat that slows down the network's performance
- Time-consuming documentation and reporting tasks that lead to audit preparation fatigue
- Lack of segmentation increases risks because adversaries able to move laterally inside the network

Are You a Novice?

- [ ] Do you look up a change and have no clue why it was made or who did it?
- [ ] Do you see a network access rule or security policy rule and wonder how it even got there?
- [ ] Do team members have no insight into why certain rules exist?
- [ ] Are people nervous about making any changes to existing rules?
- [ ] Are new rules constantly added to the top of the rule base with the least privilege approach in mind?
- [ ] Are firewalls sluggish, with rule bloat slowing things down?
- [ ] Do you or your team spend a ton of time double-checking that changes actually work?
- [ ] Do a lot of changes have to be redone?
- [ ] Are you hesitant to admit what's not getting done?

*Responding "yes" to **three or more** of the following questions likely puts you in this category.*

3 Steps to Mature Your Novice Program

At the Novice level, you need a solution that enables you to create the strong foundation necessary for scaling the network environment and digital transformation strategy.

01. Identify and Document Key Assets

By identifying key assets, you take the first step to move from an insecure "flat network" to one that has the appropriate network zones with basic segmentation, that will limit attackers' ability to move laterally across networks.

Some relevant stakeholders who should be involved when identifying "crown jewels," include:

- Infrastructure architects
- Business unit leaders
- IPAM owners
- Application managers

02. Define Desired Security Policy

With the critical assets and zones defined, you should establish the initial guidelines for user access to network segments. With these baseline segments and access policies established, you can begin setting security policies that govern only authorized access to resources. These baseline segmentation policies define how applications communicate, the networks they reside on, and who can access them.

For example, compliance and security best practices focus on creating network zones, such as an internal network or DMZ. At a minimum, the typical zones include:

- **External/public zone:** system and services requiring internet access, like web servers and email gateways, that should have strong controls limiting external threat exposure
- **Internal zone:** main internal resources for organizational users, like internal applications, file servers, and internal databases, that should be accessible only to authenticated internal users and devices
- **Sensitive/restricted zone:** most sensitive data and critical systems, like financial systems, intellectual property, and management interfaces, that are highly restricted using strict authentication and monitoring

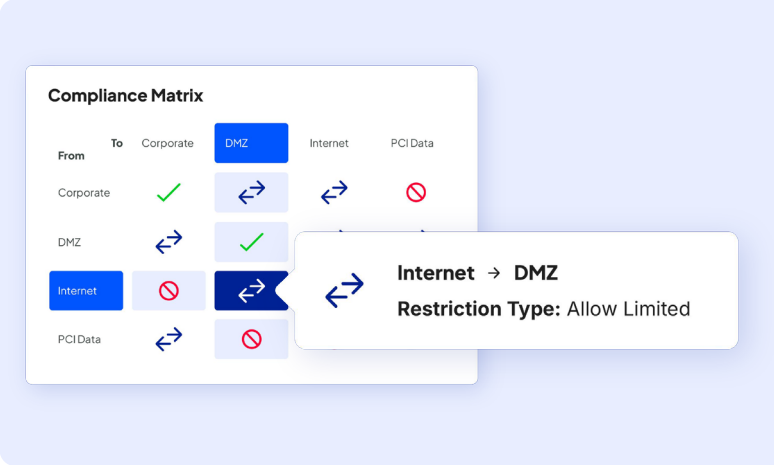
If the organization already has a spreadsheet defining these zones, you should ensure that you have visibility into different traffic and data flows for ongoing network segmentation maintenance and governance.

03. Engage with Governance/ Compliance Team

Once the organization defines its critical assets, it needs to identify its compliance requirements that may drive the controls detailed within corporate policies. For example, some compliance requirements might include one or more of the following:

- NIST
- HIPAA
- SOX
- GDPR
- PCI DSS
- ISO 27001
- NERC CIP

By building regulatory compliance templates, you can define segmentation policies and map them to align with the mandates and frameworks that govern your organization's compliance.



02 Emerging
Planning a Structured Approach

Once the organization introduces structure and reporting with initial automation, it can start to improve security policy monitoring and change management processes. At this maturity level, the organization is characterized by:

- Initial network security policy management program structure and reporting implementation
- Automation efforts begin for specific use cases, but many manual processes remain
- Focus on optimization, streamlining, and clean-up rules
- Operating reactively across teams

With simplified policy management and monitoring, the organization begins seeing some benefits, including:

- Network visibility & insights
- Reactive access & connectivity troubleshooting
- Initial network segmentation
- Basic network & policy risk management
- Manual compliance validation & audit readiness
- Security policy-driven zero trust network segmentation
- Basic automation for security policy clean up and optimization
- Early automation for security policy enforcement

Additionally, the organization now benefits at the tactical level with:

- Security policy visibility and insights across hybrid networks
- Network segmentation leading to a better zero trust-bases security posture
- Audit readiness to avoid penalties
- Vulnerability and risk prioritization
- Risk detection, prioritization, and remediation

By moving away from spreadsheets, network operations and security teams have a new level of visibility from a centralized location with metrics about things such as:

- New rules
- Modified object
- Changed rules

Indicators of this stage include:

- Centralized visibility and insights across network and security controls
- Improved understanding of the attack surface
- Faster audit preparation

Are You at the Emerging Stage?

Although organizations at this stage have less security and compliance risks, they can improve their programs by implementing more automation.

- ☐ Do you have the full context? Do you know when, what, where, or why network access requests are being made?
- ☐ Are you still hesitant to delete rules even though you are confident in making changes?
- ☐ Are your automation capabilities for rule set prioritization optimization limited?
- ☐ Are you looking to improve your firewall rule change management processes because your ticketing system fails to capture all necessary details?

*Responding "yes" to **any** of following questions likely puts you in this category*

3 Steps to Mature Your Emerging Program

Despite improved security policy management, organizations at this stage should consider how they can evolve their processes from reactive to proactive.

01. Standardize Security Policies

At this stage, most organizations have multiple firewall vendors across on-premises and multi-cloud environments. To maintain security and compliance, you want to consider standardized, vendor-agnostic policies to:

- Track policy adherence
- Identify potential security and compliance gaps
- Manage policy exceptions

An agnostic network security policy that unifies and considers the existing multi-vendor security policies gives you better visibility into and control over traffic and data flows that can undermine your security posture. Businesses should figure out:

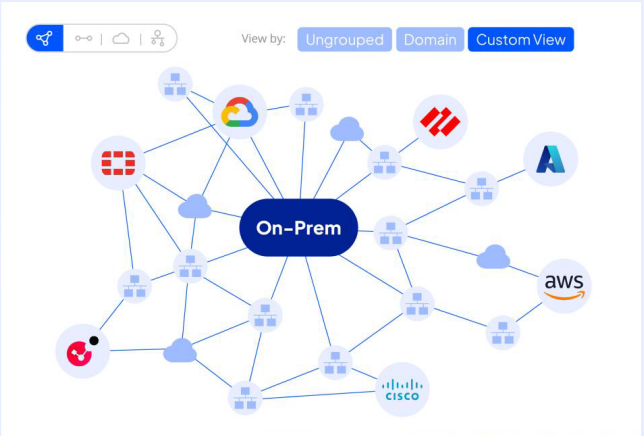
- What their "ideal state" segmentation policy looks like
- How they define their network segments
- What traffic they allowed or disallowed between network segments

By using vendor-agnostic master security policies, you centralize management of policy violations and exceptions. By centralizing control and automating access misconfiguration detection, network and cloud security teams are empowered to move towards an enterprise-wide zero-trust architecture.

02. Move Beyond Spreadsheets for Change Tracking

At this stage, tracking changes in spreadsheets becomes overwhelming, time-consuming, and error prone. To improve network security, using a single, centralized platform for all change tracking provides visibility into and governance over:

- Who made changes
- What changes were made
- When changes were made
- Why were changes made



By centralizing all change management tracking, you reduce compliance costs and create operational efficiencies. With your ruleset and change management tracking in a single location, you can create a standardized visual approach to managing security policies for building robust network governance by leveraging on-demand infrastructure and firewall rule audits to uncover violations and exceptions.

03. Integrate with Other Security and Operations Tools

Integrating network security policy management into other security solutions improves overall security and compliance. Some examples of integrations that streamline management include:

- Cloud Native Technologies
- Threat intelligence
- IT Service Management (ITSM)
- Software-defined Networking (SDN)
- Security Service Edge (SSE)
- Security Access Service Edge (SASE)
- Software-defined Wide Area Network (SD-WAN)
- IP Address Management (IPAM)
- Security Information and Event Management (SIEM)

For example, by incorporating accurate firewall data into security detections, incident response teams can reduce mean time to detect (MTTD) and mean time to respond (MTTR), ultimately reducing the financial exposure a security incident can create.

03 Advanced
Boosting Agility and Strengthening Security

At the Advanced level, the organization's automation and orchestration capabilities deliver business results quickly while strengthening the overall security posture.

At this maturity level, the organization has reliable workflows that incorporates risk analysis that include:

- Automation and orchestration that drives access changes, rule lifecycle management, and decommissioning
- Proactive compliance validation and checks before changes are made to drive continuous compliance automation
- Quick misconfiguration detection and troubleshooting across networks
- Stronger integrations with third-party tools that support more use cases

With predictable policy management and monitoring, the organization achieves the following benefits:

- Automated network policy & risk management
- Proactive network risk assessment
- Integrated security policy management across hybrid environments
- Ongoing attack surface monitoring, mitigation, and reduction
- Rule lifecycle management & least privilege
- Automated change design with least privilege principals
- Continuous compliance automation (CCA) with minimal manual intervention

Beyond these strategic benefits, the organization achieves these tactical outcomes:

- Firewall rule and policy optimization
- Attack surface reduction and advanced rule clean-up
- Network access connectivity, path analysis, and troubleshooting
- Network access management, consolidation, optimization, migration, or expansion
- Change design driven by the least privilege approach
- Continuous compliance and audit automation
- Reduced audit response times

Indicators of this stage include:

- Nearly full automation of network access
- Rapid network access troubleshooting
- Clear view of attack surface and risks
- Continuous compliance with minimal audit effort
- Fast tracking, troubleshooting, and correction of network outages

Are You at the Advanced Stage?

At this stage, companies have automation that enables them to manage network security and deliver business results quickly. Despite efficiencies, the staff may still be spending too much time on mundane tasks.

- [ ] Have you automated change processes across your firewall clusters?
- [ ] Are your network changes creating new compliance concerns or gaps in your audits?
- [ ] Do you have a process in place to validate network changes before they are made?
- [ ] Do you want to improve your network change request processes further with automation and orchestration?
- [ ] Are you managing all of your security policies across on-premise (legacy firewall) and cloud deployments (SASE) similarly or even holistically?
- [ ] Are you able to quickly troubleshoot network outages across your extended hybrid-cloud network?

*Responding "yes" to **any** of following questions likely puts you in this category*

4 Steps to Mature Your Advanced Program

With a complex, dynamic network environment, an organization should look to iterate its security program by leveraging automation and orchestration technologies. At the Advanced level, maturing network security policy management means implementing additional risk and optimization automations.

01. Automate Decommissioning Across Complex, Hybrid Environments

Decommissioning rules across hybrid network and multi-vendor environments improves network security and performance. Decommissioning rules reduce the attack surface by closing access points that are no longer needed, or simply redundant. Meanwhile, with fewer rules to process, the network speed increases. To create operational efficiencies and reduce human error risk, you can leverage automation for identifying, removing, and decommissioning:

- Duplicate objects
- Expired and unused rules and objects
- Old and unused policies
- Unauthorized or underutilized access
- Fully shadowed rules

As you begin automating and orchestrating these processes, using predefined cleanup suggestions with a security score enables you to divide these cleanups into the following types:

- **Disabled rules:** rules that never have traffic hits since they are already disabled.
- **Duplicate network objects:** matching network objects, including networks, hosts, and ranges, that have the same IP address, netmask, and zone
- **Duplicate services:** services containing the same values for characteristics that include protocol, port, source port, and others
- **Empty groups:** groups objects without any members
- **Fully shadowed and redundant rules:** rules that never have traffic hits because previous rules handle traffic
- **Unattached network objects:** Objects not used in any firewall rules or group objects
- **Unused network objects:** network objects and network object groups not used across the security policy and have no policy traffic log hits during the configured time period

02. Implement Least Privilege Change Design

When making network access changes, network administrators should implement the smaller, most efficient changes and limit them to the required enforcement points. This process ensures that users get only the access they need, no more and no less.

Network security policy automation technologies can instill trust by providing an effective and secure place where you can use the principle of least privilege as the basis of security policy changes. For example, by using these tools you can generate recommendations for:

- **Access requests:** recommending objects, rules, and other changes for implementing the access requests
- **Rule modifications:** recommendations for changing the rule base and group

03. Automate Rule Lifecycle Management

To further streamline and improve compliance and rule maintenance, organizations should automate rule lifecycle processes. Automation ensures continuous documentation and reduces the human error risks that can lead to compliance violations and security incidents.

When you automate rule lifecycle management, you can configure workflows for rule certification that document and verify the rule's purpose. By automating rule certification with a purpose-built solution, you can eve benefits like:

- Gaining visibility into a rule's status
- Knowing when the certification decision was implemented
- Knowing when to review and recertify the rule again

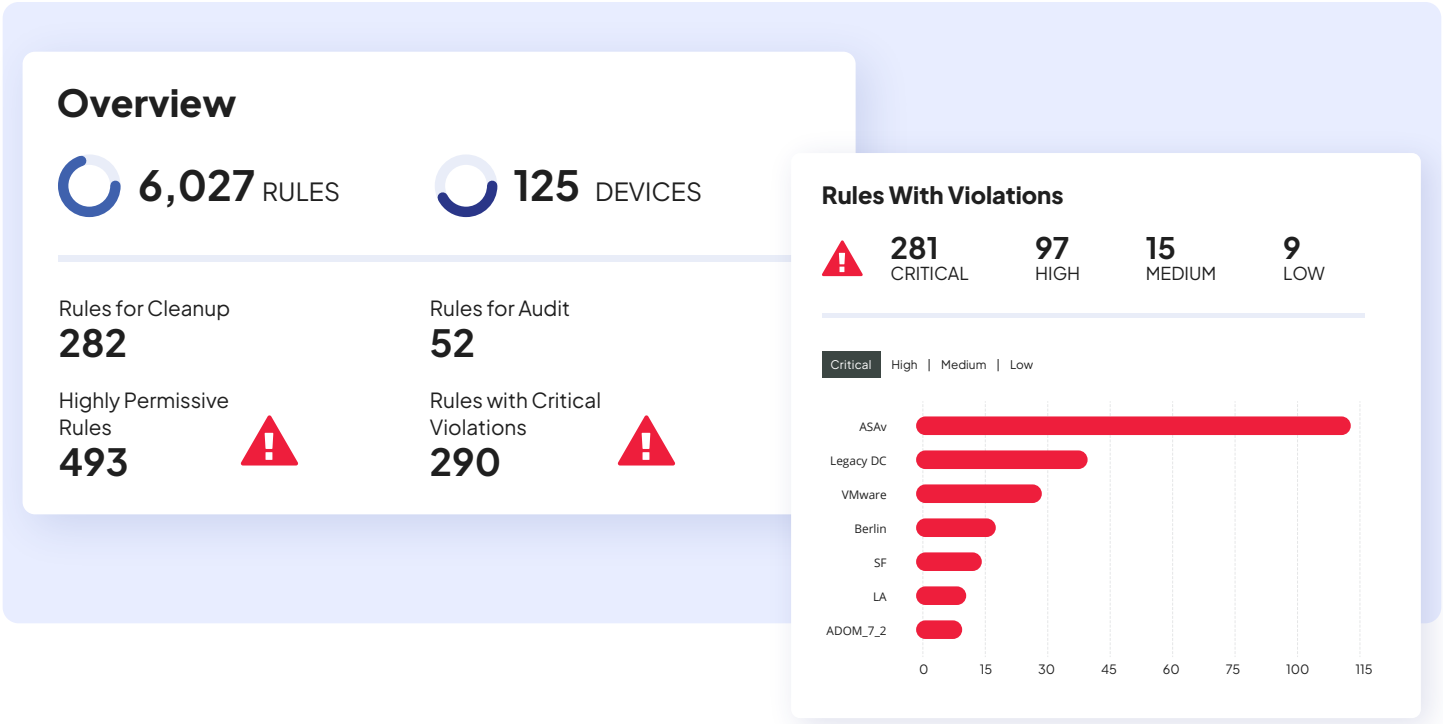
04. Build Advanced Integrations

Organizations at the Advanced level often have a robust, complex set of cybersecurity technologies. By integrating security policy management with these tools, organizations

At this level, you should add integrations with:

- IT service management (ITSM)
- Vulnerability Management Solutions
- Governance risk and compliance (GRC)
- Security orchestration, automation, and response (SOAR)
- Secure access service edge (SASE)
- Security service edge (SSE)

Integrations enable you to build robust controls across on-premises and cloud infrastructures. For example, with a single unified security policy valid across tools and technologies, organizations can enhance their SASE deployment with insights into how users access networks, allowing for more granular visibility and control.



04 Expert
Driving Innovation with Network Security Resilience

At the Expert level, organizations have comprehensive automation that enables speed, precision, and collaboration.

With visibility that allows teams to identify and troubleshoot issues in real-time, these organizations have:

- Superior visibility into network performance and security, enabling rapid troubleshooting
- Proactive risk management with automatic mitigation
- Self-service portal for instant network changes
- Compliance and risk indicators fully integrated into every change process
- Transparent collaboration between DevOps, NetSec, CloudSec, and CyberSec teams

This maturity level is characterized by reliable policy management and monitoring automation to achieve:

- Risk-informed automated network change design
- End-to-end rule lifecycle management
- Self-service automated change provisioning
- Fully integrated network security & compliance workflows
- Unified security policy management across on-premises, cloud, and applications
- Cross-team collaboration
- Rapid scalability of policy management capabilities as networks expand and grow

With a robust strategy for managing network access, these organizations also achieve tactical outcomes that include:

- Proactive risk analysis
- Rule life cycle management
- Automated change provisioning
- Application-centric policy management
- Continuously maintained network attack surface and security posture

Indicators of this stage include:

- Complete visibility and instant troubleshooting across the network
- Fully automated risk management and mitigation
- Network changes implemented in minutes via self-service
- Compliance checks and risk data embedded in all processes
- Seamless collaboration across organizational silos

Are You at the Expert Stage?

At this stage, companies have a highly advanced environment that combines visibility, automation, and collaboration in ways they previously thought were impossible.

- [ ] Do all teams, including specialized teams, have access to the same portal to reduce the time approval cycles take?
- [ ] Is automated risk mitigation an integral part of your change management process?
- [ ] Does your system predict risk and prevent compliance violations without disrupting operations?
- [ ] Do you have instant visibility into network security problems?
- [ ] Can you resolve network security and network access issues within minutes?
- [ ] Can you scale your network security policies in tandem with your expanding network?

*Responding "yes" to **all** of following questions likely puts you in this category*

3 Steps to Maintain an Expert Program

While achieving an Expert program is a challenge, maintaining it requires organizations to enhance their processes with additional, sophisticated automation.

01. Automate Rapid Change Provisioning

With automation that pushes policy changes life across management devices, firewall devices, cloud devices, and SASE technologies, organizations with complex network environments can accelerate the implementation of the policy recommendations from their automation.

This uplevels the end-to-end rule life cycle management by reducing the number of change windows that involve engineers. With rapid change provisioning, you can:

- Save policy changes to a single device, like firewall device or security group
- Apply and enforce changes as soon as they are provisioned
- Commit changes from management devices to all child firewall devices
- Configure scheduled change windows for automatic provisioning
- Reduce human error with automation and orchestration

02. Implement App-Centric Policy Management

By leveraging application centric security policy management, organizations gain visibility into the communications between applications and services across the network. Since using app-centric policy management translates the application owner's intentions to the network, it means that network operations and security teams no longer need to focus solely on IP addresses, they can now understand the business context of the network access request and act accordingly. With the ability to understand dependencies between applications, you can rapidly troubleshoot application connectivity and dependent application connectivity, including insight into potential misconfigurations for additional oversight and visibility into their cloud security posture management.

If you have a well-organized network topology, you can view your entire network from a functional perspective. This visibility bridges the gap between application owners with no network experience and network administrators. With a central console driven by a unified network view, you can troubleshoot for and mitigate risks related to misconfigurations that can cause business application outages.

Organization gains benefits like:

- Real-time visibility into business applications, including connectivity requirements, status, and open change tickets
- End-to-end application connectivity views, including configured connections and diagnostic tool for fixing issues
- Collaboration across network operations and application teams
- Automation for creating, updating, or decommissioning an application connection to define, implement, monitor, and maintain application connectivity more efficiently

03. Ensure High Availability

At this level, organizations can focus on leveraging a high availability architecture to support their business continuity and disaster recovery programs.

By building in redundancy mechanisms with Tufin, organization can prevent a single point of failure by:

- Replicating data to prevent service outages
- Implementing failover to keep services running
- Fixing issues without worrying about having service disruptions

Making the Business Case for Maturing Network Security Policy Management

Using insight into your organization's current maturity level, you can assess the effectiveness of your current tooling and identify the next steps on your journey.

As organizations continue to seek solutions to their cybersecurity and compliance challenges, they need to map business outcomes to their purchases carefully. These technology investments help you manage current issues, but they should respond to future security needs, too.

As you learn, grow, and scale your network, you need to consider how a network security policy management solution:

- Eases current pain points
- Enables your maturity journey into the future

When evaluating different solutions, you should start by considering the business use cases that matter most to your organization and how their functionalities help you achieve those goals. For example, Tufin's suite of solutions was purpose-built around business process enablement so that security, network, and IT teams could gain efficiencies while improving network security and compliance.

Business Agility

Digital transformation is a never-ending process. To remain competitive, businesses continue to add new applications to their networks. However, network and security teams struggle to manage:

- Configuration requirements early in the provisioning process
- Manual, error prone processes
- Time-to-business value when struggling with connectivity issues
- Security and compliance across a hybrid network

With Tufin's security policy management capabilities, orchestration, and automation, organizations can reduce application connectivity management efforts by 75%. By automatically generating policies, network, security, and IT teams can collaborate to accelerate their cloud network expansion project schedules. With enhanced visibility into network topology and security configurations, you can identify configuration and security requirements earlier in the provisioning process. This shift enables you to reduce time-consuming and costly errors and rework.

Security

Your organization's digital transformation strategy often complicates security. With multiple firewall vendors across their on-premises and cloud infrastructure, network operations and security teams face challenges that include:

- Managing vendor-specific security policy configurations
- Time-consuming processes for designing and management network and cloud segmentations and micro segmentations
- Lack of real-time visibility into network topology, including assets, applications, services, and traffic
- Time-consuming and error-prone change management processes
- Inability to identify and remove unnecessary firewall rules

By unifying security operations with Tufin's automated risk analysis capabilities, you can reduce the risk of breach due to vulnerabilities by 80%. Leveraging Tufin's security policy rule management and cleanup capabilities, security and network operations teams can rapidly identify gaps and risks, including overly permissive policies and exposed, risky ports across the hybrid cloud network.

Compliance

Security challenges parallel and impact the organization's compliance program. For network operations and security teams, key regulatory compliance mandates define baselines security requirements. As the company expands its business operations, it may need to achieve compliance with multiple regulations or industry standards, including:

- NIST 800-53
- PCI DSS v.4.0
- ISO 27001
- NERC CIP v.5

In dynamic network environments, network operations and security teams face compliance challenges like:

- Diverse, vendor-specific firewall rules that can lead to compliance violations
- Establishing and enforcing least privilege access across various vendor-defined access controls
- Time-consuming audit preparation and reporting processes
- Lack of proactive risk analysis during the change management process
- Documenting rule and policy changes and maintaining a firewall audit history

By centralizing and automating network security policy management with Tufin, you can gain the following compliance efficiencies:

- 85% for ongoing rule maintenance
- 95% for audit preparation and reporting

Tufin simplifies and documents adherence with internal policies and compliance mandates. With vendor agnostic Unified Security Policies (USPs) mapped to multiple compliance standards, organizations can rapidly generate security attestation and reporting. By leveraging change management risk analysis and workflows, organizations can proactively identify non-compliant changes to maintain continuous compliance across their dynamic networks.

Operational Efficiency

At their core, manual, error-prone processes create operational inefficiencies that cost the organization money. Without automation, many organizations face operational issues that can include:

- Additional overhead as security staff tries to manage growing workloads
- Focusing on repetitive rule management activities rather than high-value, strategic work
- Time-consuming processes for identifying and removing unnecessary or risky rules

To understand Tufin's financial value, you should consider how operational efficiencies drive labor cost savings. Leveraging automation across the security policy design, testing, implementation, change management, and deployment processes can help organizations achieve up to:

- $5 million saving for network management, rule maintenance, and audit preparation/reporting
- $3.1 million associated with reduced data breach and user downtime risks
- $715,000 arising from faster provisioning

Tufin

A Scalable Security Policy Management Solution for Maturing Your Program

Regardless of an organization's security policy management maturity level, Tufin's suite of solutions can help it grow and evolve. Our scalable services enable organizations to begin their journey then grow with them as they need additional capabilities.

With Tufin Orchestration Suite (TOS), organization's get unmatched visibility for easy troubleshooting across the entire hybrid network. Our Topology Map enables a single view with Path Analysis that allows network operations and security teams to investigate all devices along a network path potentially impacting connectivity.

Our centralized, hybrid-cloud, multi-vendor management solution provides a unified platform that streamlines network and application connectivity while ensuring precise configuration and fast, efficient handling of complex infrastructure changes. Organizations gain comprehensive network security that anticipates risks, integrates security into firewall changes, and adeptly manages security zones across devices.

To see how Tufin can help you mature your network security, contact us for a demo today

tufin