THE SECURITY POLICY MANAGEMENT MATURITY MODEL

UNDERSTANDING THE LEVELS OF ENTERPRISE READINESS FOR MANAGING NETWORK SECURITY POLICIES

An AlgoSec Whitepaper

MANAGE SECURITY **AT THE SPEED OF BUSINESS**

Executive Summary

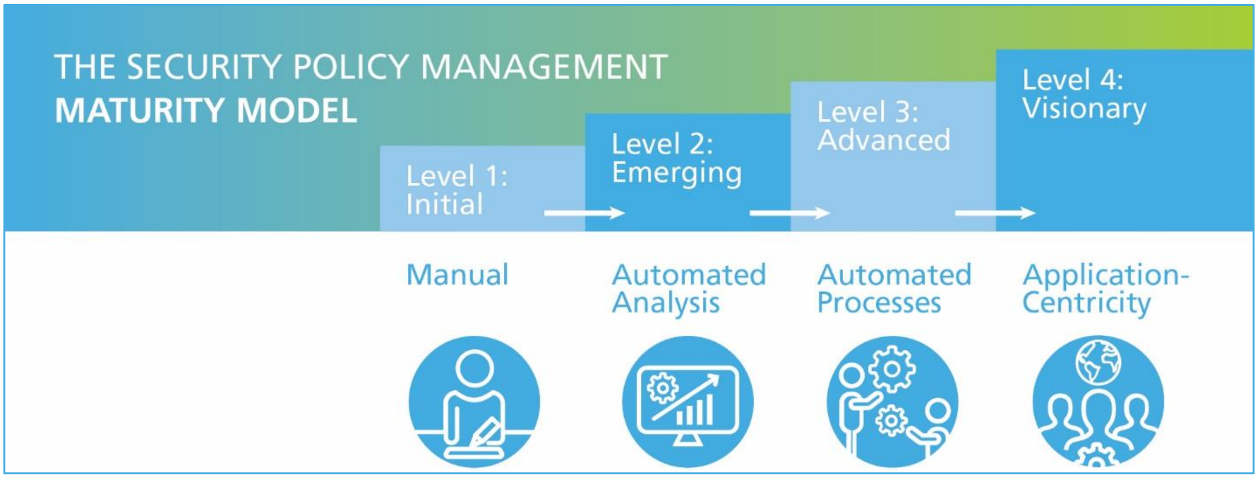
Increased network complexity together with demands on business agility have made the traditional, manual approach to managing security policies untenable. As network security devices continue to evolve, so too must security policy management. Security policies are in place to not only block malicious traffic, but also to enable connectivity and business productivity.

There are many challenges involved with managing the security policy. It requires optimizing policies, understanding application connectivity requirements, ensuring more granular control and orchestrating policies through a streamlined process that enables stakeholders to quickly respond to changing business needs. Each organization's security policy management maturity level depends on the level of analysis, automation and process that can involve security administrators, network operations, compliance officers, application owners and senior management.

This paper examines the four stages of the security policy management model – manual, automated analysis, automated processes and finally application centric and provides ways to:

- Identify an organization's maturity level
- Explore each level's strengths and weaknesses
- Compare gaps in current practice with the ideal approach
- Provide a framework for prioritizing activities to move up the curve

The security policy management maturity model can help organizations recognize their current environment and provide a roadmap for improvement in their security policy management. As organizations move farther along the maturity model they will experience significant operational efficiencies and improvements in agility, while also being able to ensure a more secure and compliant network environment.



Level 1: Initial - Manual

Organizations at the Initial level of the maturity model take a mostly or entirely manual approach to security policy management. These organizations lack the visibility, control and processes to quickly respond to changing business needs, and cannot easily demonstrate compliance or understand their risk posture. Common challenges for these organizations are time-consuming, manual processes, lack of visibility into policies, and poor change management.

Here are typical characteristics of a company taking a manual approach:

Limited understanding of why each firewall rule exists: Typically the "knowledge" of why a rule was created or changed is in the brains of the administrators. If the admin can't remember the reason or if they leave the company, there is no history to review and it is much harder to troubleshoot firewall-related issues, reduce risk and outages caused by rule changes.

Limited visibility of impact on network traffic: Organizations at this level often do not have an understanding of how the security policy impacts traffic flowing to and from the network which turns planning and troubleshooting into extremely complex tasks. Being able to generate an accurate map of network topology requires a major undertaking – and usually has gaps.

Change management is manual and error prone: Organizations at the initial stages of security policy management have no sound way to enforce the security change process. This means multiple ways of processing changes, increased risk of misconfiguration and non-compliance, no process for decommissioning application connectivity, and overall a much slower process that impedes business agility.

Time-consuming audits: Regulatory compliance as well as internal mandates result in frequent firewall audits. Organizations at this level spent days and even weeks preparing their firewall for audits manually. Achieving compliance in this manner is not only time-consuming, but also short lived, as frequent changes can cause organizations to fall out of compliance shortly after the audit.

RECOMMENDATIONS FOR ORGANIZATIONS AT THIS LEVEL

1. Review (or create) documentation for firewall rules
2. Get an accurate picture of your network traffic so you understand what your policy is actually doing
3. Define your ideal change management process
4. Establish regular projects to clean up firewall and router rules and ACLs
5. Review risk analysis and compliance processes and assess benefits of automation

Bloated firewall rule sets: Security policies typically grow in size and complexity over time. Organizations at “Level 1” have bloated rule sets – rules added, but never deleted - because of the fear of causing an outage or a security risk by removing a rule.

Manual risk analysis of the firewall policy: According to Gartner, “More than 95% of firewall breaches are caused by firewall misconfigurations, not firewall flaws.” Many organizations don’t understand the risks of enabling or disabling certain rules.

Level 2: Emerging – Automated Analysis

Organizations that have reached this level have addressed the visibility challenges by automating policy analysis and tracking changes across all of the devices in the network. However automation efforts are still mostly tactical and are limited to point-in-time efforts such as audits or cleanup projects. Emerging organizations have not automated change management and cannot ensure continuous compliance.

Here are typical characteristics of a company that automates analysis:

Automated monitoring and alerting of policy changes: Visibility improvements from the Initial level are dramatic, with automated tracking and notifications when rules are changed, which is helpful for audits and for identifying the origin when troubleshooting connectivity or risk issues.

Automated audit reports for point-in-time compliance: Organizations can automatically generate reports that demonstrate compliance with a myriad of regulations, standards and/or corporate policies, instead of conducting manual audits that can take weeks for just one firewall. While audits are faster and more accurate, organizations typically fall out of compliance in between audits due to frequent changes.

Automated policy optimization & risk analysis: Unused rules and objects, covered, duplicate, expired rules and much more can be quickly discovered. Rules may also be reordered for optimal performance. Risk and severity in the firewall policy is now understood, with the ability to identify overly broad rules where "ANY" is in the SRC, DEST, SERVICE, APP or USER fields and tighten those rules without impacting business requirements.

Change management still manual and error-prone: There may be process review and improvements underway, but still little to no process automation or firewall-aware intelligence that can significantly improve the speed and accuracy of making changes. Many changes need to be redone and out-of-process changes are performed, which lead to trouble.

Lack of understanding of business impact from security changes: The lack of understanding of the business impact of security changes during data center application migrations to public, private or hybrid clouds often results in outages to a critical application or possibly the network during data center application migrations to public, private or hybrid clouds.

RECOMMENDATIONS FOR ORGANIZATIONS AT THIS LEVEL

1. Make sure security and network teams are aligned and agree on change management processes
2. Integrate risk and compliance analysis to the change process *BEFORE* making the change
3. Measure the time required for each step of a change request to identify bottlenecks
4. Conduct reconciliation between requests and actual changes made to identify out-of-process changes
5. Assess the value of automation as part of a firewall and network aware change process

Level 3: Advanced – Automated Process

“Advanced” companies have automated the security change management process, bringing together security and network teams to process changes more quickly and with greater accuracy and to ensure continuous compliance. However, automation and visibility is not extended to application owners. “Advanced” companies may still struggle to understand business requirements and make the security infrastructure “work for the business”.

Here are typical characteristics of a company taking an automated approach:

More agile security change workflow: Now security and network operations teams aligned for better response to dynamic business needs. Change requests are processed more quickly and accurately through automated workflows that eliminate what were previously manual, time-consuming processes. Redundant change requests are immediately eliminated by comparing change requests with the rule(s) are already in place and automatically closing those change request tickets.

Continuous compliance and accountability: Organizations can ensure that every change request is automatically analyzed for risk BEFORE the change is made, allowing involved stakeholders to make informed decisions about changes that affect risk and compliance levels. Advanced organizations can measure every step of the security change workflow to demonstrate compliance and ensure service level agreements are attained.

Out-of-process changes are discovered: Organizations at this level can eliminate out-of-process changes by automatically matching each change request with the change that was actually performed.

Limited visibility of business impact of security changes: At this level of the maturity model, while security and network operations teams are in sync, application owners are not looped into the security change process which causes key requirements to get “lost in translation”. There is little to no understanding of the impact a connectivity change may have on other business applications.

Basic documentation of application connectivity needs (E.g. spreadsheets): Organizations at this level typically have spreadsheet-level documentation of business application connectivity requirements. Regardless, there is little visibility and control of these requirements and their relation with the security policy. As a result many organization experience outages or impaired network performance as a result of application-related rule changes.

RECOMMENDATIONS FOR ORGANIZATIONS AT THIS LEVEL

1. Review processes for documenting application connectivity requirements
2. Assess gaps between application and network teams relating to the security and network infrastructure
3. Review processes for decommissioning applications and related unused firewall rules
4. Examine options for making business owners “own the risk” and the vulnerabilities in their applications
5. Assess tools which provide application-centric approaches to managing the network security policy

Vulnerabilities are not prioritized by business impact: While organizations have vulnerability management solutions in place, the long lists of vulnerabilities produced is too much for any business to adequately address. Vulnerability information is typically presented for IP addresses and servers, and not in the context that business owners can understand.

Level 4: Visionary

Instead of looking at these devices from strictly a firewall/security perspective, "Visionary" organizations are making decisions from the perspective of critical business applications in the data center. All key stakeholders across security, network operations and application teams have visibility of the business requirements and the security implications and are aligned through streamlined and automated business processes.

Characteristics of an organization taking an application-centric approach include:

Faster security provisioning of data center applications: Organizations at this level can quickly and securely provision connectivity for business applications to ensure maximum service delivery and availability. By automatically translating application connectivity requirements into the necessary firewall rules, triggering the appropriate change requests and embedding rich analysis capabilities, organizations can simplify and accelerate policy changes and enable security to keep up with the "speed of business".

Full understanding of application connectivity needs: "Visionary" organizations have a dynamic alternative to documenting and maintaining application connectivity requirements in spreadsheets. Linking the application connectivity needs to the security policy, the associated rules and the impacted devices is a key component of an application-centric approach to managing the security policy.

Application, security and operations teams are aligned: "Visionary" organizations have implemented an application-centric approach to security policy management that accommodates each constituency and provides the means for them to "speak the same language".

Secure decommissioning of applications, removing rules no longer in use: With an application-centric approach, organizations can accurately identify and remove access rules for decommissioned applications, without impacting the accessibility of other applications. This improves security without impacting availability and performance.

BENEFITS FOR ORGANIZATIONS AT THIS LEVEL

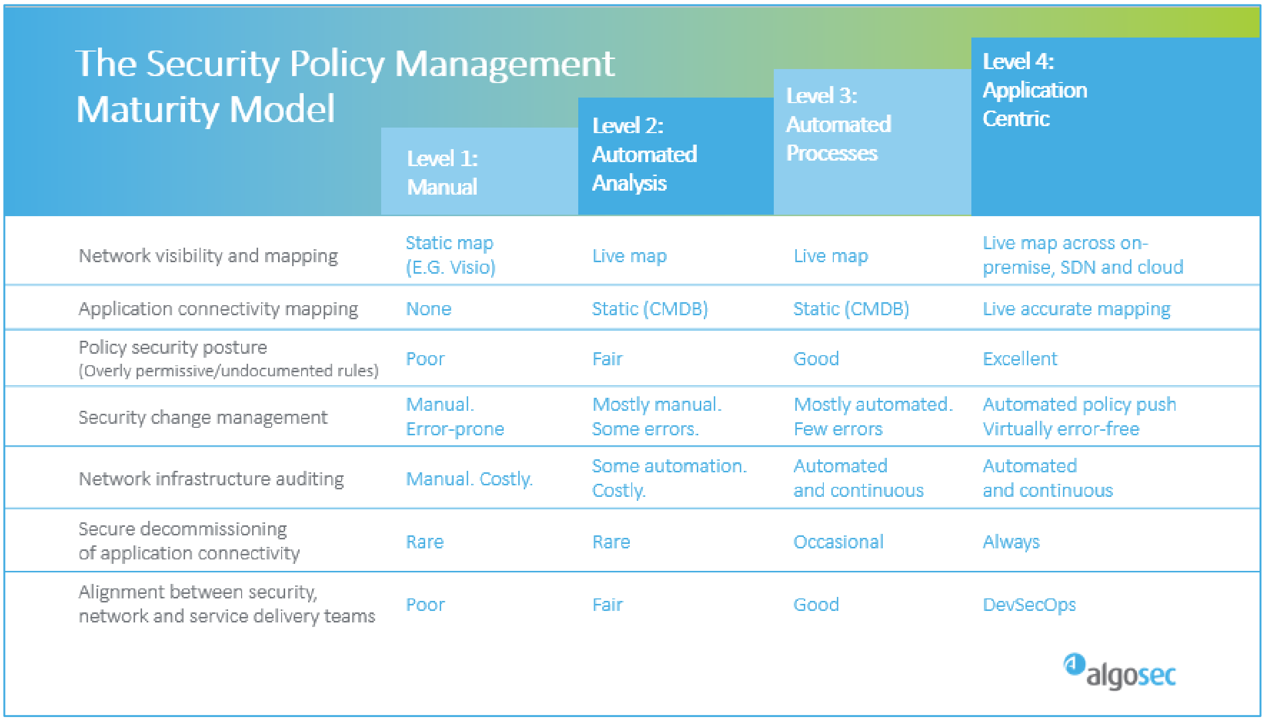
1. Improved application availability – even during a data center migration
2. Faster service delivery
3. Alignment across IT, security and the business
4. Tighter security policies to improve defense against cyber-attacks
5. Real ROI and more time, resources and budget to focus on strategic initiatives

Elimination of application outages due to firewall misconfigurations: As new applications are added - or the connectivity requirements for existing ones are modified – "Visionary" organizations can calculate the underlying firewall rules/changes that are needed and initiate the corresponding change process. Since application outages are often a result of poor firewall rule changes, being able to identify the impact to an organization's applications of proposed changes to the network, such as server migrations or new routing and segmentation schemes is significant.

The business can “own the risk”: Organizations at this level can integrate with existing vulnerability scanners and map vulnerabilities with their related data center applications, including their servers and complex connectivity requirements. Aggregating vulnerability information into an application-centric view enables all risks associated with a line of business to be displayed and prioritized accordingly. Now the business can be accountable and “own the risk”.

Conclusion

Rising network complexity and increased demands on business agility are rapidly hindering the traditional approach to managing security policies. Security policies are in place to not only block malicious traffic, but also to enable connectivity. As network security devices continue to evolve, so too must security policy management. This means more optimized policies, more granular control and a more streamlined process that enables organizations to quickly respond to changing business needs. The security policy management maturity model can help organizations recognize their current environment and provide a roadmap for improvement.



The Security Policy Management Maturity Model

	Level 1: Manual	Level 2: Automated Analysis	Level 3: Automated Processes	Level 4: Application Centric
Network visibility and mapping	Static map (E.G. Visio)	Live map	Live map	Live map across on-premise, SDN and cloud
Application connectivity mapping	None	Static (CMDB)	Static (CMDB)	Live accurate mapping
Policy security posture (Overly permissive/undocumented rules)	Poor	Fair	Good	Excellent
Security change management	Manual. Error-prone	Mostly manual. Some errors.	Mostly automated. Few errors	Automated policy push Virtually error-free
Network infrastructure auditing	Manual. Costly.	Some automation. Costly.	Automated and continuous	Automated and continuous
Secure decommissioning of application connectivity	Rare	Rare	Occasional	Always
Alignment between security, network and service delivery teams	Poor	Fair	Good	DevSecOps

The impact that IT can have on the business is undeniable. Ensuring that all key stakeholders are involved as appropriate in key decisions can improve performance and availability of business-critical applications, close security gaps, and dramatically increase responsiveness to changing business requirements. The end game is a more secure, more agile business, with a real security policy management ROI attached.

About AlgoSec

AlgoSec simplifies, automates and orchestrates security policy management to enable enterprise organizations and service providers to manage security at the speed of business. Over 1,500 of the world's leading organizations, including 15 of the Fortune 50, rely on AlgoSec to optimize the network security policy throughout its lifecycle, to accelerate application delivery while ensuring security and compliance. AlgoSec is committed to the success of each and every customer, and provides the industry's only money-back guarantee.

For more information visit http://www.AlgoSec.com or visit our blog.

Global Headquarters
65 Challenger Road,
Suite 320
Ridgefield Park
NJ 07660, USA
+1-888-358-3696

EMEA Headquarters
80 Coleman Street
London EC2R 5 BJ
United Kingdom
Tel: +44 207-099-7545

APAC Headquarters
10 Anson Road, #14-06
International Plaza
Singapore 079903
+65-3158-2120

AlgoSec.com