WHITE PAPER

The Case and Criteria for Application-Centric Security Policy Management

Sponsor: AlgoSec

Author: Mark Bouchard

AimPoint Group

keeping IT on target

Executive Summary

As the security policies required to protect today's networks continue to grow in volume and complexity, manual approaches for managing them are rapidly becoming untenable. Such methods are simply too cumbersome, inefficient, and error-prone, resulting in increased cost, risk, and the inability for IT Security and Operations to keep pace with the needs of the business.

What today's organizations need instead is an enterprise-class solution that helps automate all phases of the policy management lifecycle, from initial creation and implementation to ongoing monitoring, change processing, and auditing. But even that is not enough. Just as many critical IT functions have evolved to become application-centric, so too must security policy management. Ideally, it should be possible to manage security policies from the perspective of the business applications they are intended to support, as opposed to requiring an intimate knowledge of nebulous, network-level attributes. This is essential to bridging the divide that exists between network, security, and applications personnel in today's IT departments, and holds the key to maximizing application availability, reducing risk from unauthorized access, and unlocking greater degrees of IT agility.

Why Automated Security Policy Management is Necessary

The effectiveness of an organization's primary network defenses (e.g., firewalls, proxy servers, and other network security gateways) depends considerably on the policies that are configured to govern their operation. However, implementing and maintaining these policies so that they optimally balance the needs of the business with the need to limit risk is becoming increasingly challenging. This is due in part to:

Growing scope and complexity. For most organizations new business applications are being added and/or changed at a rapid pace; more users must be supported as access and services are extended to a greater number of contractors, partners, and customers; and more controls need to be accounted for as defenses get more sophisticated (e.g., with next-generation firewalls).

Escalating rates of change. To enhance their competitiveness, today's businesses are striving to be more adaptive. This is forcing IT to become more responsive, and driving the adoption of practices and technologies (e.g., storage, server, and network virtualization) that promote flexibility and enable rapid change. From a network security perspective, the result is the need to accommodate a steadily increasing frequency and volume of associated policy changes.

Continuing to rely on disjointed, manual approaches to policy management under these conditions is simply too costly, and not just in terms of the labor involved. Other drawbacks include the increased potential for:

- Botched service delivery, in the form of access outages and less than timely troubleshooting/recovery;
- Security incidents, stemming from policy errors or omissions;
- Audit findings, and any accompanying penalties and repercussions; and
- Keeping IT (and the business) from being as adaptive as it would like to be.

Why Security Policy Management Also Needs to be Application-Centric

The obvious answer is for enterprises to implement a solution that automates security policy management. However, this only begins to address the challenges at hand. Another fundamental problem facing today's security teams is that the techniques still utilized by traditional firewall/policy management tools are woefully out-of-date and poorly aligned with the rest of IT, not to mention the needs of the business.

Although networks and applications were once simple enough such that "allow service XYZ from IP Address 1 to IP Address 2" was sufficient, that is no longer the case. There are now far more enterprise applications – with complex, multi-tier architectures, far-flung components, and convoluted, underlying communication patterns – driving today's network security policies. In addition, any individual "communication" may need to traverse multiple policy enforcement points, while individual rules may, in turn, support multiple distinct applications. The net result is a far more complex scenario characterized by hundreds to thousands of policies, with many potential but not always obvious inter-dependencies, configured across tens to hundreds of devices, in support of equally as many business-critical applications.

By failing to evolve to address this increasing complexity, traditional solutions have also forced IT to adopt a less than ideal approach where connectivity requirements for business applications are specified and maintained in completely separate repositories. The challenge with these information stores – which include CMDBs, homegrown databases, manually maintained spreadsheets and even the heads of individual administrators themselves – is that they are often out-of-date, unreliable, difficult to access, and in no way connected to or correlated with the policies that are ultimately configured. In addition, the process of sharing, interpreting, and accurately translating whatever information they do contain into effective policies is entirely too cumbersome and error prone.

What today's organizations require to address this situation is a solution that takes an application-centric approach to security policy management – one that incorporates application connectivity management as an integral component and enables the derivative policies to be managed from the perspective of the applications they support (rather than the networking attributes ultimately used to enforce them). Additional reasons for pursuing such a solution include the following:

- Applications (and data) are all that matter to the business. Indeed, to demonstrate and maintain its relevance to the business, IT has already made the transition to application-centric language and practices in many areas (e.g., application performance monitoring, application delivery controllers/networking). A similar up-leveling is long overdue for information security which, for the most part, continues to rely too heavily on nebulous networking attributes and terminology.
- Adding an application-oriented dimension can effectively "bridge the gaps" between the different constituencies within IT – application developers/owners, networking, security, and operations – each of which has a role to play when it comes to security policy management, and each of which has its own language, responsibilities, and agenda (see sidebar).
- Having applications be the focal point provides a layer of abstraction that conveniently helps mask the growing complexity of today's security policies.

Overall, a solution that enables an application-centric approach to security policy management should help to further increase efficiency, avoid errors, and ensure that the connectivity needs of the business are met in an accurate and timely manner.

Bridging the Application-Networking-Security Divide

Within IT, each department typically has its own objectives and even language that it uses. Application developers and owners focus on features/functions, the different tiers/components of their applications, data, and ensuring broad accessibility. In many cases, they aren't even concerned with underlying server hardware any more. The networking team concentrates on routing and connectivity while communicating in terms of subnets, IP addresses, ports and protocols. And security professionals are consumed with threats, vulnerabilities, risks, compliance and - much to the chagrin of the application folks – strictly limiting which users have access to which resources.

This all works well enough for the most part. It's when these groups have to work together that problems arise. All too often the differences in responsibilities and terminology result in key requirements getting "lost in translation" - or simply being ignored due to a lack of understanding. As a result, applications wind up "broken" or inaccessible, security is unnecessarily compromised, and network performance is adversely impacted. Having a solution that incorporates an application-centric approach to security policy management alleviates this situation by accommodating each IT constituency and providing the means to fluidly translate and navigate between their different requirements.

What Enterprises Should Look for in a Solution

Being application-centric is clearly an important consideration when it comes to selecting a solution for automated security policy management. But what exactly does this mean in terms of supported feature and functions? And what about the underlying policy management capabilities that are needed to even have a solution in the first place? The following sections answer these questions in the form of essential criteria that enterprises can use to evaluate candidate solutions.

Core Policy Management Capabilities

The foundation for a modern policy management solution is its ability to deliver comprehensive, intelligent policy analysis and extensive automation.

Comprehensive, intelligent policy analysis.

Essential functionality for managing and optimizing an organization's configured security policies includes:

- Topology intelligence, for understanding device relationships and network paths;
- Policy cleanup and tightening, to remove unnecessary and/or overly permissive rules;
- Policy tuning, to re-order rules for optimal performance;
- Risk assessment, to flag rules that run counter to acknowledged best practices; and,
- Baseline configuration compliance (i.e., define and manage to configuration baselines).

Extensive automation. With the need to process a growing number of policy changes - often on a daily basis - automation has become absolutely critical. Highly detailed and fully customizable change management workflows are essential in this regard, and also serve as a "fail-proof" mechanism for ensuring accuracy. Additional opportunities for a solution to help improve efficiency and responsiveness include:

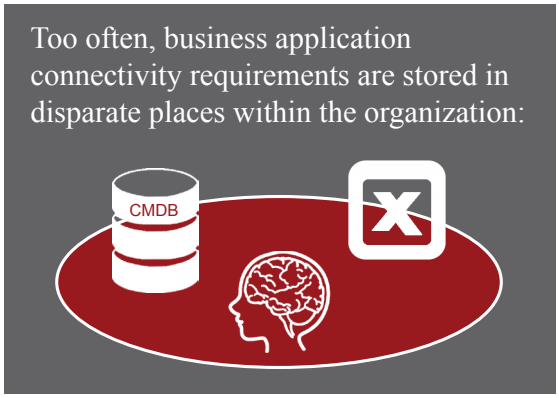
- Automated change assessment, to check proposed policy changes for risk, compliance, and redundancy red flags;
- Automated change vectoring, to identify specifically which devices are affected;
- Automated policy implementation, to actually re-configure affected devices;
- Automated change validation, to establish correct implementation and close corresponding tickets; and,
- Automated audit and compliance reports.

Application-Centric Management Model

As discussed, a solution that takes an application-centric approach to security policy management should deliver greater efficiency and effectiveness than one that relies solely on networking details, concepts, and terminology. In this regard, having an application-oriented front end for security policy management is only a starting point. Emphasis on business applications should be exhibited across all major aspects of the solution.

Application connectivity portal.

The solution should include - as a tightly integrated component - a "living" alternative to traditional static methods for documenting and maintaining application connectivity requirements. And although these requirements will ultimately be the basis for detailed security rules, the language and objects used to define them should be simple and familiar to application developers, owners, and business management. For example, domain/common names - such as app1.company.com and dbase1.company.com - should be sufficient to specify the source and destination of a given application flow.



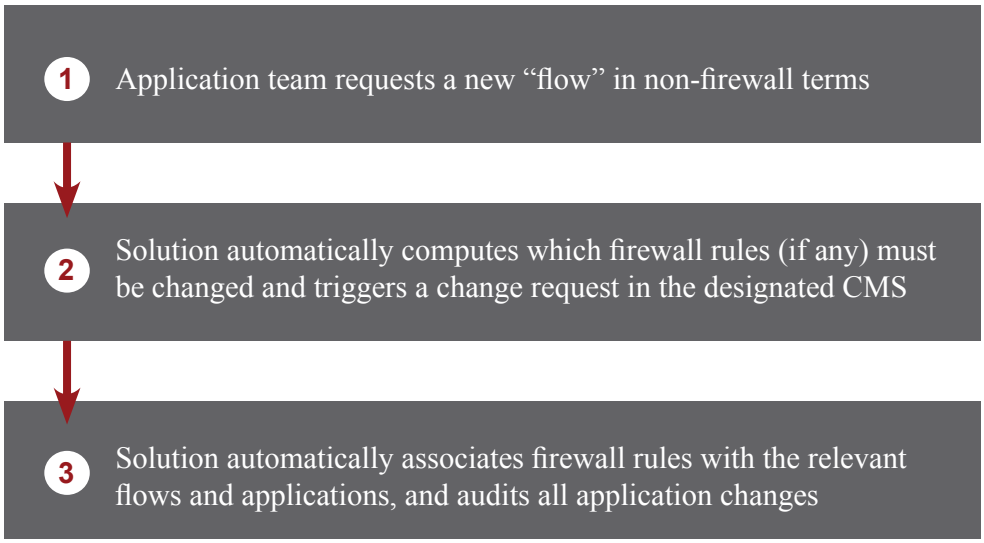
In addition, administrators should not be limited to re-creating all of an organization's application flows from scratch. Instead, multiple methods should be supported for populating the portal in the first place. These include the ability: (a) to import application connectivity data from existing sources, such as spreadsheets, homegrown databases, and popular CMDBs, and (b) to "learn" connectivity requirements based on automated analysis of the current configurations for an organization's firewalls, routers, and other relevant devices. Another related feature to look for is the ability to define dependencies between different applications (so they can be accounted for during policy analysis).

Application-centric analysis. As new applications are added - or the connectivity requirements for existing ones are modified - it should be possible to have the solution not only calculate the underlying firewall rules/changes that are needed, but also initiate the corresponding change management workflow. Additional, application-centric analysis capabilities to evaluate include the ability 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;
- Accurately identify/remove access rules for decommissioned applications, without impacting the accessibility of other applications; and,
- Identify the impact to an organization's applications of proposed changes to access rules - for example, in response to newly discovered threats or vulnerabilities.

The value of secure application decommissioning, in particular, cannot be over-stated. For many organizations, retired applications are a major contributor to bloated rule sets that increase management complexity and needlessly expose the enterprise to greater risk.

Example Flow for Adding or Editing an Application



Application-centric visibility and reporting. With application-centricity ideally extending across the entire policy management lifecycle, it should also be exhibited in the form of application-connectivity status monitoring and the ability to visually depict application flows and connectivity outages. Equally important are application-specific linkages that allow users to quickly navigate/correlate between application connectivity definitions and any and all associated rules, tickets, analyses, visualizations, and reports. Additional, essential features related to reporting include the ability to:

- Automatically compile an audit trail that provides a complete historical record of all changes to an application's connectivity requirements and underlying rules, along with all related change tickets; and,
- Facilitate a device-level compliance audit, where business justification is effectively provided for each of a device's access rules by tying them to the applications they support.

What Enterprises Stand to Gain

The evolution to application-centric security policy management promises to deliver numerous significant benefits for today's enterprises. These include:

Faster service delivery, enabling greater overall IT/business agility. Streamlined processes, numerous embedded analysis features, and an automated workflow dramatically simplify and accelerate policy changes and other aspects of policy management, thereby enabling IT security to keep pace with the increasing "speed of business".

Improved application availability. Process automation and an application-centric management model substantially reduce the potential for manually introduced errors and misunderstandings regarding application connectivity requirements, respectively. This leads to fewer incidents where misconfigured security devices incorrectly block access to business applications, or between their various components.

Improved efficiency of IT/security interactions and operations. With an application-centric approach, application connectivity requirements and resulting security policies are maintained together in a single, consolidated tool. Moreover, linkages between the two not only eliminate ambiguity and enable smoother communication between different IT departments, but also simplify previously time consuming and otherwise challenging tasks – such as cross-team troubleshooting and identifying the impact that policy and network architecture changes will have on individual applications.

Reduced risk and potential for compliance audit findings. Unnecessary or overly permissive access rules can be eliminated or tightened, respectively, based on a more accurate and accessible understanding of related application connectivity requirements. At the same time, providing the business justification for each policy/rule becomes a simple matter of pointing to the application(s) it supports.

Increased credibility and relevance of IT Security in the eyes of business management. Focusing on, better enabling, and communicating in terms of what matters most to the business – applications and services – goes a long way toward demystifying what the security department does and convincing the "powers that be" that the security team is on the right track (and not just an impediment to the business).

Conclusion

The bottom line is that rising IT complexity and agility are rapidly rendering traditional approaches to network security policy management untenable. In response, enterprises need to embrace the evolution to application-centric security policy management. Implementing a corresponding solution not only introduces a much-needed dose of automation, but also does so in a way that bridges the gaps that are prevalent between network, security, and applications personnel in today's IT departments. The net result is increased performance and availability of business-critical applications, reduced risk from leftover connectivity requirements that are never cleaned up, enhanced responsiveness to changing business conditions, and better assurance that IT Security is/remains aligned with the needs of the business.

About the Author

Mark Bouchard, CISSP, is the founder of AimPoint Group, an IT research and analysis company specializing in information security, compliance management, application delivery, and infrastructure optimization. A former META Group analyst, Mark has analyzed business and technology trends across a wide range of information security, networking, and systems management topics for more than 15 years. A veteran of the U.S. Navy, he is passionate about helping enterprises address their IT challenges and has assisted hundreds of organizations worldwide meet both tactical and strategic objectives.