algosec

# The network security policy management lifecycle:

## How a lifecycle approach improves business agility, reduces risks, and lowers costs

# Introduction

**IT security organizations today are judged on how they enable business transformation and innovation. They are tasked with delivering new applications to users and introducing new technologies that will capture new customers, improve productivity and lower costs. They are expected to be agile so they can respond faster than competitors to changing customer and market needs.**

Unfortunately, IT security is often perceived as standing in the way of innovation and business agility. This is particularly true when it comes to provisioning business application connectivity. When an enterprise rolls out a new application or migrates an application to the cloud it may take weeks or even months to ensure that all the servers, devices and network segments can communicate with each other, and at the same time prevent access to hackers and unauthorized users.

But IT security does not have to be a bottleneck to business agility. Nor is it necessary to accept more risk to satisfy the demand for speed.

The solution is to manage application connectivity and network security policies through a structured lifecycle methodology. IT security organizations that follow the five stages of a security policy management lifecycle can improve business agility dramatically without sacrificing security.

**A lifecycle approach not only ensures that the right activities are performed in the right order, it provides a framework for automating repeatable processes, and enables different technical and business groups to work together better.**

**In this whitepaper, we will:**

**01** Review the obstacles to delivering secure application connectivity and business agility.

**02** Explore the lifecycle approach to managing application connectivity and security policies.

**03** Examine how the activities at each stage of the lifecycle can help enterprises increase business agility, reduce risks, and lower operating costs.

# Why is it so hard to manage application and network connectivity?

**Top IT managers sometimes view security policy management as something routine, just part of the "plumbing." In reality, delivering secure connectivity requires mastering complex data center and cloud infrastructures, coping with constant change, understanding esoteric security and compliance requirements, and coordinating the efforts of multiple technical and business teams.**

## Application connectivity is complex

The computing infrastructure of even a medium-sized enterprise includes hundreds of servers, storage systems, and network security devices such as firewalls, routers and load balancers. Complexity is magnified by the fact that many application components are now virtualized. Moreover, hybrid cloud architectures are becoming common. And since networking concepts differ profoundly between physical and cloud-based networks, unified visibility and control are very difficult to obtain.

## Change never stops

Business users need access to data – fast! Yet every time a new application is deployed, changed or migrated, network and security staffs need to understand how information will flow between the various web, application, database and storage servers. They need to devise application connectivity rules that allow traffic while preventing access from unauthorized users or creating gaps in their security perimeters.

## Security and compliance require thousands of application connectivity rules

Many security policies are required to manage network access and protect confidential data from outside attackers and from unauthorized access by users or employees. In a typical enterprise, customers and businesses are only allowed to access specific web servers in a "demilitarized zone." Some applications and databases are authorized for all employees, while others are restricted to specific departments or business units or management levels.

Government regulations and industry standards require severely controlled access to credit card and financial information, Personally Identifiable Information (PII),

Protected Health Information (PHI) and many other types of confidential data. Security best practices often require additional restrictions, such as limiting the use of protocols that can be used to evade security controls.

To enforce these policies, IT security teams need to create and manage thousands, tens of thousands, and sometimes even hundreds of thousands of firewall rules on routers, firewalls and other network and security devices in order to comply with the necessary security, business and regulatory requirements.

## Technical and business groups don't communicate

After application delivery managers outline the business-level requirements of new or modified applications, network and security architects must translate them into network flows that traverse various Web gateways, web servers, application servers, database servers and document repositories. Then firewall administrators

and other security professionals have to create firewall rules that allow the right users to connect to the right systems, using appropriate services and protocols. Compliance and risk management officers also get involved to identify potential violations of regulations and corporate policies.

These processes are handicapped by several factors:

- Each group speaks a different business or technical language.
- Information is siloed, and each group has its own tools for tracking business requirements, network topology, security rules and compliance policies.
- Data is often poorly documented.
- Often network and security groups are brought in only at the tail end of the process, when it is too late to prevent bad decisions.

# The lifecycle approach to managing application connectivity and security policies

**Most enterprises take an ad-hoc approach to managing application connectivity. They jump to address the connectivity needs of high-profile applications and imminent threats, but have little time left over to maintain network maps, document security policies and firewall rules, or to analyze the impact of rule changes on production applications. They are also hard-pressed to translate dozens of daily change requests from business terms into complex technical details.**

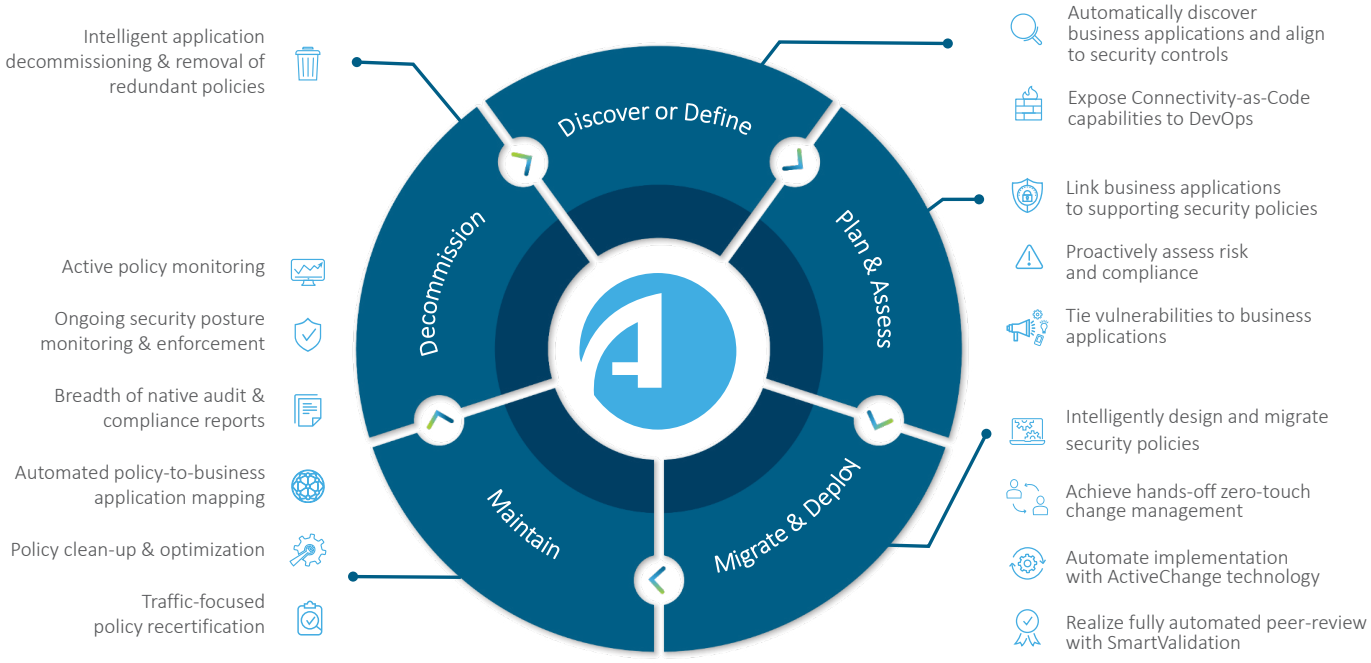
### The costs of these dysfunctional processes include:

- Loss of business agility caused by delays in releasing applications and improving infrastructure.
- Application outages and lost productivity caused by errors in updating rules and configuring systems.
- Inflexibility, when administrators refuse to change existing rules for fear of "breaking" existing information flows.
- Increased risk of security breaches, caused by gaps in security and compliance policies, and by overly
- permissive security rules on firewalls and other devices.
- Costly demands on the time of network and security staff, caused by inefficient processes and high audit preparation costs.

IT security groups will always have to deal with complex networks and constantly changing applications. But given these challenges, they can manage application connectivity and security policies more effectively using a lifecycle framework such as the one illustrated in Figure 1.

This lifecycle approach captures all the major activities that an IT organization should follow when managing change requests that affect application connectivity and security policies, organized into five stages.

### Figure 1: The network security policy lifecycle



## Structure activities and reduce risks

A lifecycle approach ensures that the right activities are performed in the right order, consistently. This is essential to reducing risks. For example, failing to conduct an impact analysis of proposed firewall rule changes can lead to service outages when the new rules inadvertently block connections between components of an application. While neglecting to monitor policies and recertify rules can result in overly permissive or unnecessary rules that facilitate data breaches.

A structured process also reduces unnecessary work and increases business agility. For example, a proactive risk and compliance assessment during the Plan & Assess stage of the lifecycle can identify requirements and prevent errors before new rules are deployed onto security and network devices. This reduces costly, time- consuming and frustrating "fire drills" to fix errors in the production environment.

A defined lifecycle also gives network and security professionals a basis to resist pressures to omit or shortchange activities to save time today, which can cause higher costs and greater risks tomorrow.

## Automate processes

The only way IT organizations can cope with the complexity and rapid change of today's infrastructure and applications is through automation.

A lifecycle approach to security policy management helps enterprises structure their processes to be comprehensive, repeatable and automated.

When enterprises automate the process of provisioning security policies, they can respond faster to changing business requirements, which makes them more agile and competitive. By reducing manual errors and ensuring that that key steps are never overlooked, they also avoid service outages and reduce the risk of security breaches and compliance violations.

Automation also frees security and networking staffs, so they have time to spend on strategic initiatives, rather than on routine "keep the lights on" tasks.

Ultimately, it permits enterprises to support more business applications and greater business agility with the same staff.

## Enable better communication

A lifecycle approach to security policy management improves communication across IT groups and their senior management. It helps bring together application delivery, network, security, and compliance people in the Discover & Visualize and Plan & Assess stages of the lifecycle, to make sure that business requirements can be accurately translated into infrastructure and security changes.

The approach also helps coordinate the work of network, security and operations staffs in the Migrate & Deploy, Maintain and Decommission stages, to ensure that deployment and operational activities are executed smoothly. And it helps IT and business executives communicate better about the security posture of the enterprise.

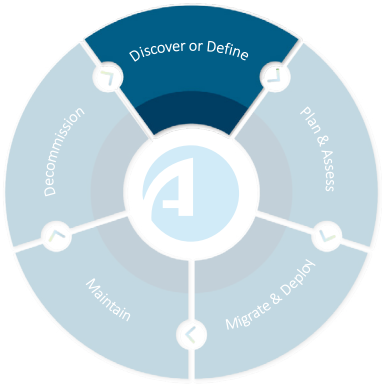
## Document the environment

In most enterprises security policies are poorly documented. Reasons include severe time pressures on network and security staff, and tools that make it hard to record and share policy and rule information (e.g., spreadsheets and bug tracking systems designed for software development teams). The result is minor time savings in the short run ("we'll document that later when we have more time") at the cost of more work later, lack of documentation needed for audits and compliance verification, and the greater risk of service outages and data breaches.

Organizations that adopt a lifecycle approach build appropriate self-documenting processes into each step of the lifecycle.

We will now look at how these principles and practices can be implemented in each of the five stages of a security policy management lifecycle.

# Stage 1: Discover & visualize




Automatically discover business applications and align to security controls

Expose Connectivity-as-Code capabilities to DevOps

The first stage of the security policy management lifecycle is Discover & Visualize. This phase is key to successful security policy management. It gives IT organizations an accurate, up-to-date mapping of their application connectivity across on-premises, cloud, and software-defined environments. Without this information, IT staffs are essentially working blind, and will inevitably make mistakes and encounter problems down the line.

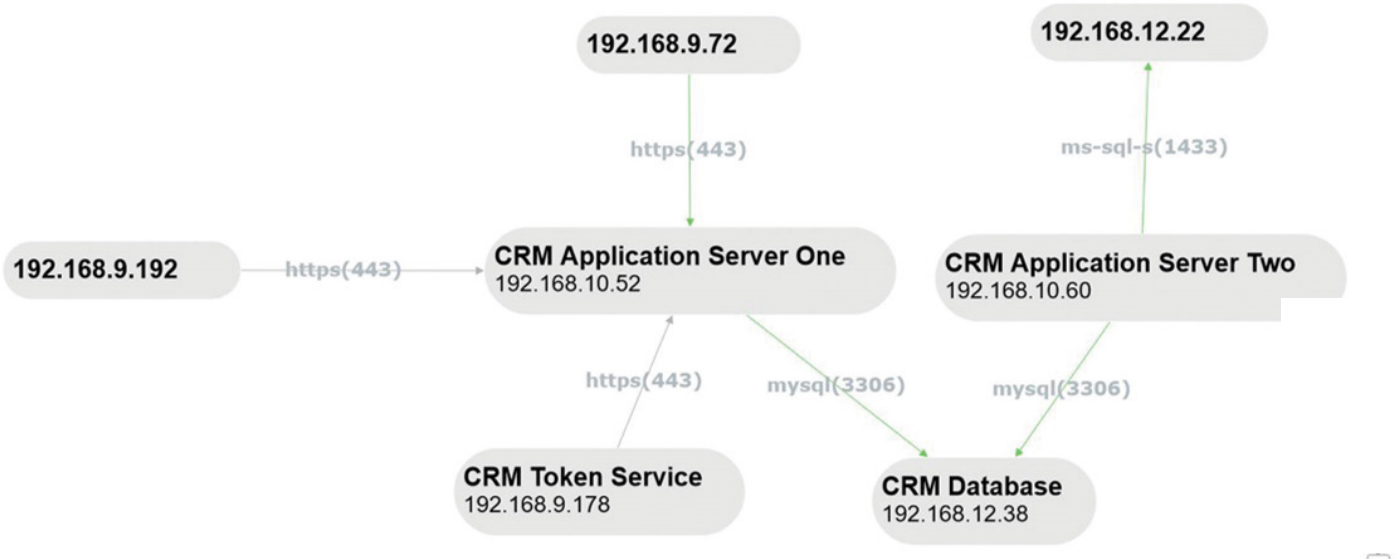
While discovery may sound easy, for most IT organizations today it is extremely difficult to perform. As discussed earlier, most enterprises have hundreds or thousands of systems in their enterprise infrastructure. Servers and devices are constantly being added, removed, upgraded, consolidated, distributed, virtualized, and moved to the cloud. Few organizations can maintain an accurate, up-to-date map of their application connectivity and network topology, and it can take months to gather this information manually.

Fortunately, security policy management solutions can automate the application connectivity discovery,

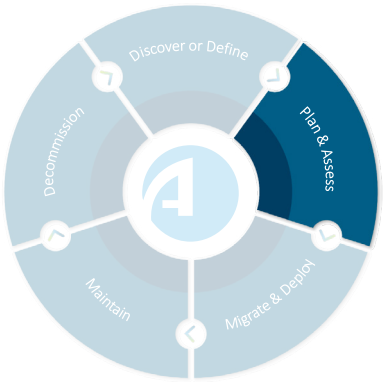
mapping, and documentation processes (see Figure 2). These products give network and security staffs an up-to-date map of their application connectivity and network topology, eliminating many of the errors caused by out-of-date (or missing) information about systems, connectivity flows, and firewall rules.

In addition, the mapping process can help business and technical groups develop a shared understanding of application connectivity requirements.

**Figure 2: Auto discover, map and visualize application connectivity and security infrastructure.**



# Stage 2: Plan & assess




- Link business applications to supporting security policies
- Proactively assess risk and compliance
- Tie vulnerabilities to business applications

Once an enterprise has a clear picture of its application connectivity and network infrastructure, it can effectively start to plan changes.

The Plan & Assess stage of the lifecycle includes activities that ensure that proposed changes will be effective in providing the required connectivity, while minimizing the risks of introducing vulnerabilities, causing application outages, or violating compliance requirements.

Typically, this stage involves:

- Translating business application connectivity requests, typically defined in business terms, into networking terminology that security staff can understand and implement.
- Analyzing the network topology, to determine if the requested changes are really needed (typically 30% of requests require no changes).
- Conducting a proactive impact analysis of proposed rule changes to understand in advance how they will affect other applications and processes.
- Performing a risk and compliance assessment, to make sure that the changes don't open security holes or cause compliance violations (see Figure 3).
- Assessing inputs from vulnerabilities scanners and SIEM solutions to understand business risk.

Many organizations perform these activities only periodically, in conjunction with audits or as part of a major project. They omit impact analysis for "minor" change requests and even when they perform risk assessments, they often focus on firewall rules and ignore the wider business application implications.

Yet automating these analysis and assessment activities and incorporating them as part of a structured lifecycle process helps keep infrastructure and security data up to date, which saves time overall and prevents bad decisions from being made based on outdated information. It also ensures that key steps are not omitted, since even a single configuration error can cause a service outage or set the stage for a security breach.

Impact analysis is particularly valuable when cloud- based applications and services are part of the project as it is often extremely difficult to predict the effect of rule changes when deployed to the cloud.

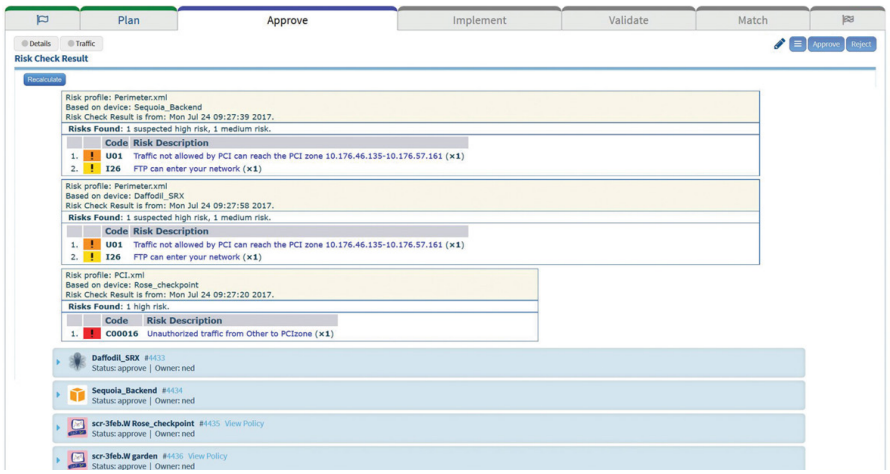
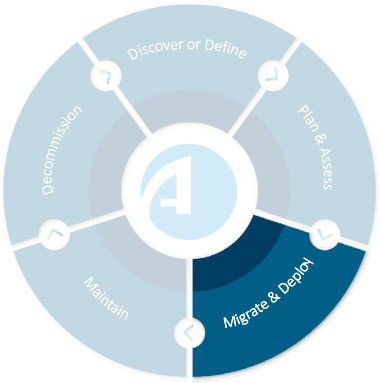



**Figure 3: Proactively assess risk and compliance for each security policy change**

# Stage 3: Migrate & deploy




- Intelligently design and migrate security policies
- Achieve hands-off zero-touch change management
- Automate implementation with ActiveChange technology
- Realize fully automated peer-review with SmartValidation

The process of deploying connectivity and security rules can be extremely labor-intensive when it involves dozens of firewalls, routers, and other network security devices. It is also very error-prone. A single "fat-finger" typing mistake can result in an outage or a hole in the security perimeter. Security policy management solutions automate critical tasks during this stage of the lifecycle, including:

- Designing rule changes intelligently based on security, compliance and performance considerations.
- Automatically migrating these rules using intuitive workflows (see Figure 4).
- Pushing policies to firewalls and other security devices, both on-premises and on cloud platforms – with zero touch if no exceptions are detected (see Figure 5).
- Validating that the intended changes have been implemented correctly. Many enterprises overlook the validation process and fail to check that rule changes have been pushed to devices and activated successfully. This can create the false impression that application connectivity has been provided, or that vulnerabilities have been removed, when in fact there are time bombs ticking in the infrastructure.

By automating these tasks, IT organizations can speed up application deployments, as well as ensure that rules are accurate and consistent across different security devices. Automated deployment also eliminates the need to perform many routine maintenance tasks and therefore frees up security professionals for more strategic tasks.

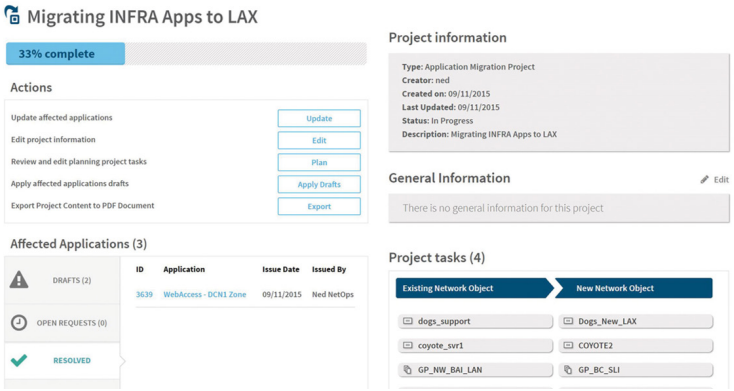



**Figure 4: Automate firewall rule migration through easy-to-use workflows.**

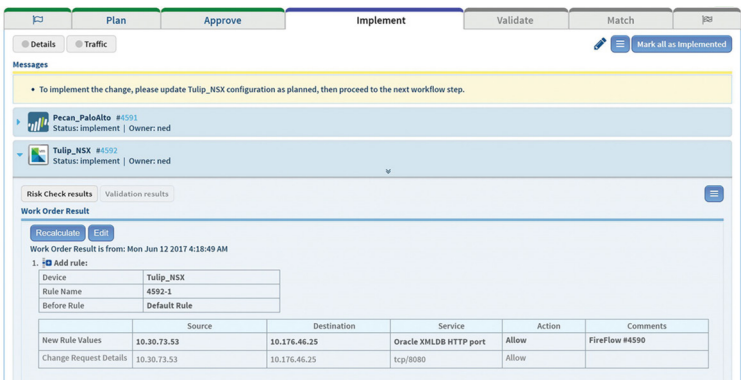
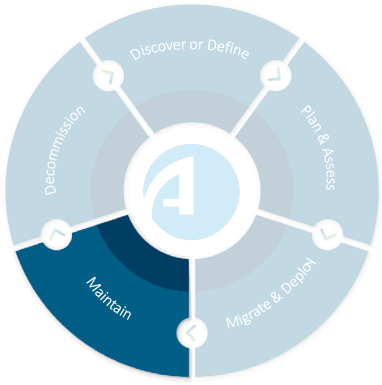



**Figure 5: Deploy security changes directly onto devices with zero touch**

# Stage 4: Maintain




- Active policy monitoring
- Ongoing security posture monitoring & enforcement
- Breadth of native audit & compliance reports
- Automated policy-to-business application mapping
- Policy clean-up & optimization
- Traffic-focused policy recertification

In the rush to support new applications and technologies, many IT security teams ignore, forget or put off activities related to monitoring and maintaining their security policy – despite the fact that most firewalls accumulate thousands of rules and objects which become out-of-date or obsolete over the years.

Typical symptoms of cluttered and bloated rulesets include:

- Overly permissive rules that create gaps in the network security perimeter which cybercriminals can use to attack the enterprise.
- Excessively complicated tasks in areas such as change management, troubleshooting and auditing.
- Excessive audit preparation costs to prove that compliance requirements are being met, or conversely audit failures because overly permissive rules allow violations.
- Slower network performance, because proliferating rules overload network and security devices.
- Decreased hardware lifespan and increased TCO for overburdened security devices.

Cleaning up and optimizing security policies on an ongoing basis can prevent these problems (see Figure 6). Activities include:

- Identifying and eliminating or consolidating redundant and conflicting rules.
- Tightening rules that are overly permissive (for example, allowing network traffic from ANY source to connect to ANY destination using ANY protocol).
- Reordering rules for better performance.
- Recertifying expired rules based on security and business needs (see Figure 7 on the next page).
- Continuously documenting security rules and their compliance with regulations and corporate policies.

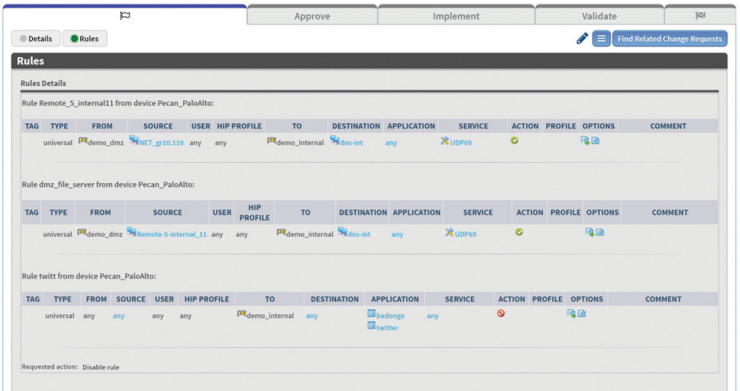
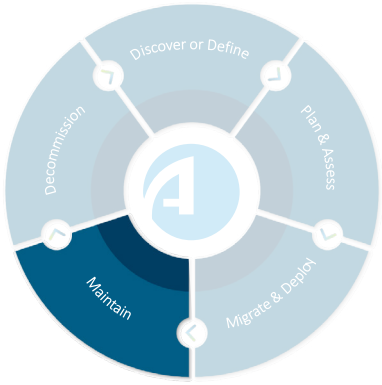



**Figure 6: Automatically clean up and optimize security policies**

# Stage 4: Maintain (continued)




- Active policy monitoring
- Ongoing security posture monitoring & enforcement
- Breadth of native audit & compliance reports
- Automated policy-to-business application mapping
- Policy clean-up & optimization
- Traffic-focused policy recertification

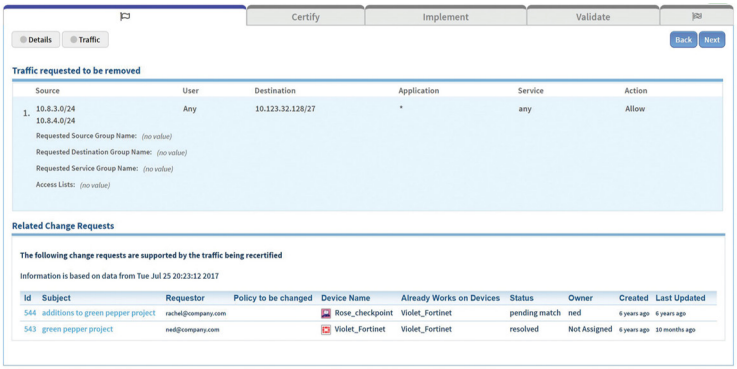
Automating these maintenance activities helps IT organizations move towards a "clean," well-documented set of security rules so they can prevent business application outages, compliance violations, security holes, and cyber-attacks. It also reduces management time and effort.

Another key benefit of ongoing maintenance of security policy rules is that it significantly reduces audit preparation efforts and costs by as much as 80%.

(see Figure 8).

Preparing firewalls for a regulatory or internal audit is a tedious, time-consuming and error- prone process. Moreover, while an audit is typically a point-in-time exercise, most regulations today require enterprises to be continually compliant, which can be difficult to achieve with bloated and ever-changing rule bases.

**Figure 7: Review and recertify rules based on security and business needs**



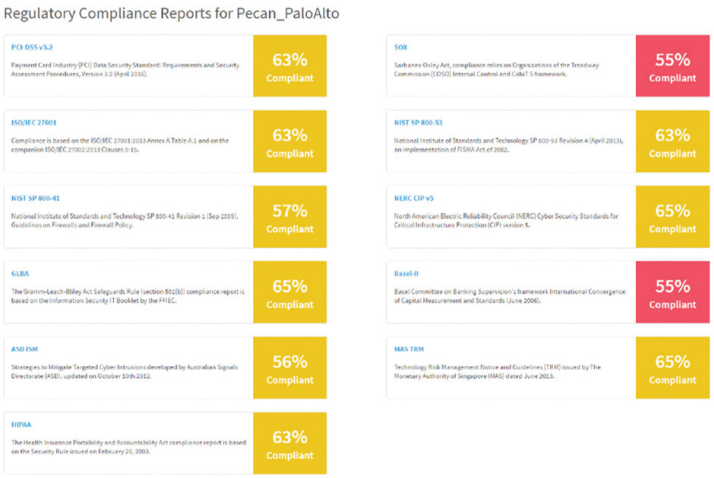
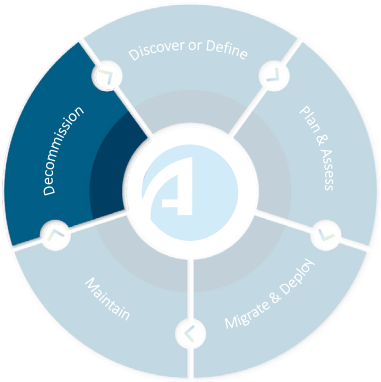




**Figure 8: Significantly reduce audit preparation efforts and costs with automated audit reports.**

# Stage 5: Decommission




Intelligent application decommissioning & removal of redundant policies

Every business application eventually reaches the end of its life. At that point some or all of its security policies become redundant. Yet when applications are decommissioned, their policies are often left in place, either from oversight or out of fear that removing policies could negatively affect active business applications. These obsolete or redundant security policies increase the enterprise's attack vector and add clutter, without providing any business value.

A lifecycle approach to managing application connectivity and security policies reduces the risk of application outages and data breaches caused by obsolete rules. It provides a structured and automated process for identifying and safely removing redundant firewall rules as soon as applications are decommissioned, while verifying that their removal will not impact active applications or create compliance violations (see Figure 9).

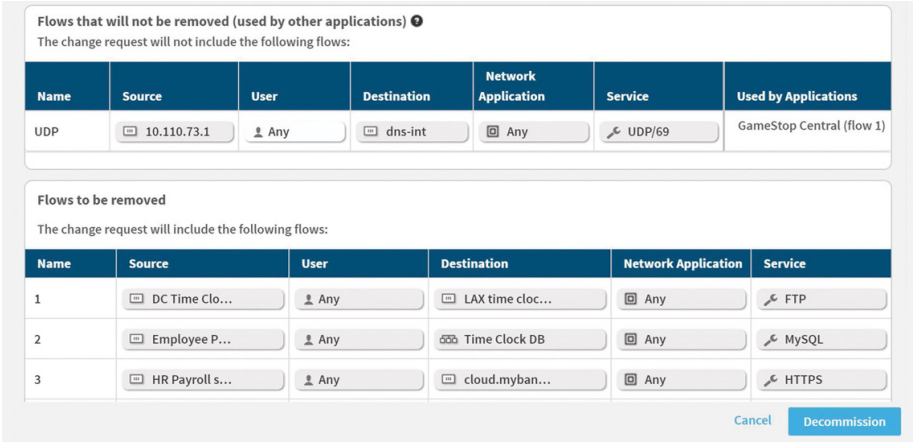


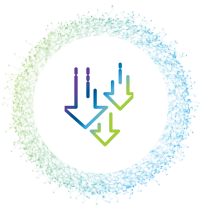

**Figure 9: Automatically and safely remove redundant firewall rules when applications are decommissioned**

# Summary

**Network and security operations should never be a bottleneck to business agility and must be able to respond rapidly to the ever-changing needs of the business. The solution is to move away from a reactive, fire-fighting response to business challenges and adopt a proactive lifecycle approach to managing application connectivity and security policies that will enable IT organizations to achieve critical business objectives such as:**

Increasing business agility by speeding up the delivery of business continuity and business transformation initiatives.

Reducing the risk of security breaches caused by gaps in security and compliance policies and overly permissive security rules.



Reducing the risk of application outages due to errors when creating and deploying connectivity and security rules.

Freeing up network and security professionals from routine tasks so they can work on strategic projects.

AlgoSec.com