

Secure application connectivity.
Anywhere.

An application-centric approach to firewall rule recertification: Challenges and benefits

An AlgoSec Whitepaper

Introduction

Firewall rules support applications or processes that require network connectivity to and from specific servers, users and networks. Every year these rules need to be reviewed and recertified as part of on-going security best practices.

The rationale for rule recertification is:

- Security:** Retaining unused/unnecessary rules on your firewall exposes your network to attacks
- Compliance:** PCI-DSS regulation best practices recommend periodic reviews of firewall rules
- Optimization:** The more rules you have, the greater the burden on firewall performance. Firewall bloat also makes firewall rulesets harder to manage.

In the past, the only way to recertify a rule was to manually review the comments field in each firewall rule. This field should, at a minimum, include the name of the original requester of the rule as well as the rule's purpose. Assuming this information was indeed included within the rule, this method is extremely error-prone and hard to manage.

A more efficient and effective method to manage the firewall rule recertification process is to take an application-centric approach. This means taking a step back and identifying all the relevant business applications that each rule supports, enabling you to then sift through and review the firewall rules quickly and easily. If the application still exists and has not been modified, all of its rules should still apply and can be recertified. If, however, the application no longer exists or has changed, the firewall rules can be removed.

This paper provides an overview of the rule recertification process – from both the firewall rule perspective and the application perspective. It also explains how to implement an application-centric approach to rule recertification and highlights some of the key benefits.

Why firewall rules become redundant

There are several potential reasons why a firewall rule becomes redundant:

An application is decommissioned

Many firewall rules become redundant when the application that relies on them to function is no longer in use, yet the firewall rules are not removed, even though they no longer serve any purpose.

An application is upgraded and uses different services/ports

This is a common scenario. For example, a desktop application is upgraded to a web application and a new rule is created to support port 8080 network connectivity instead of updating the existing rule, which remains in the rule base even though it no longer serves any purpose.

An endpoint is moved to a different datacenter

This may occur as part of an upgrade, cloud migration project or simply a hardware refresh. Again, new rules are created to support connectivity but the old rules remain in place unnecessarily.

Managing/removing unnecessary firewall rules

Companies typically handle the rule recertification process either on an ongoing or project basis:

Ongoing review by expiration dates

Many organizations set an expiration date for each rule, and every week a firewall administrator looks at the rules that are about to expire in the upcoming week and decides either to extend the expiration date or remove the rule. Using this method, the rule recertification process is an ongoing activity rather than a point-in-time project.

In rare cases, organizations do not review the rules that are about to expire and wait to hear from the end-user when an application doesn't work. Only then do they update the expiration date of the relevant rules.

Project-based periodic review

Some organizations prefer to handle rule recertification on a project basis, where firewall administrations review and validate all firewall rules from all firewalls at the same time.

The recertification process typically includes four main steps for each rule:

1. Review the firewall logs and determine when the rule was last used
2. Read the comments to see who requested the rule and which application it serves
3. Validate that the application is in use with the relevant contact
4. Remove the rule or extend the expiration date

Whichever method is used, an automated network security management solution can handle much of this process, saving significant time, effort and minimizing errors. It should provide visibility into each firewall across your estate, including the rules, network objects and configurations. In addition to the time savings, this ensures that all firewalls and their rules are reviewed and not overlooked.

Additionally, the automation solution should provide a detailed report of all the unused rules giving you an initial target list of rules to review. Some network security policy management solutions include the ability to set expiration dates for rules and automatically alerts the user when it needs to be reviewed and recertified. Through the solution's change management capabilities, you should be able to automatically implement the removal of the firewall rules (and roll-back changes in the event of a mistake), and get a full audit trail that automatically documents all these activities.

An application-centric approach to firewall rule recertification

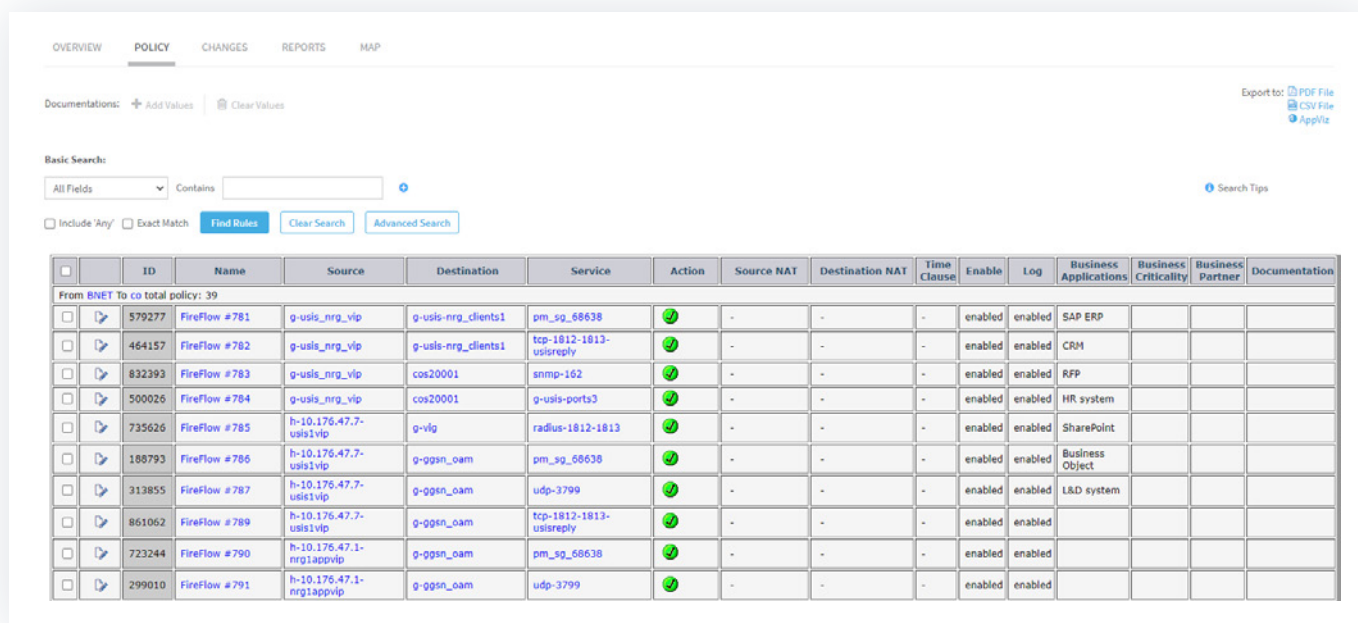
Irrespective of whether performed manually or using an automation solution, rule recertification is a time-consuming process – especially in enterprise organizations where there may be hundreds or even thousands of firewalls, each with hundreds or thousands of firewall rules. Taking an application-centric approach to rule recertification significantly streamlines the process.

Firewall rules exist to support business applications, so it is far easier to identify the rules that need to be recertified based on whether they support an existing application. If the application exists and has not been modified, all its rules should still apply and therefore can be immediately recertified. If the application has been removed, its rules are no longer relevant and can be removed. If an application has been altered, you will need to further research its rules to determine the status of its firewall rules.

Discovering applications and their rules

In order to take an application-centric approach to rule recertification, you first need to identify all of the applications in your network. This can be done manually: you can approach all of the different business units in your organization and ask them which applications they use or are responsible for. Alternatively you can use a solution such as AlgoSec, that can automatically discover and map application connectivity. As part of this process, you will likely discover applications on your network that are not being used and can be decommissioned together with their rules.

Next, you need to identify all firewalls and their rules and associate each rule to the application it serves. Again, this can be done manually – a very complex and time-consuming process – or using a solution which does this automatically, such as AlgoSec (see figure 1).



The screenshot shows the AlgoSec interface with a table of firewall rules. The table has columns for ID, Name, Source, Destination, Service, Action, Source NAT, Destination NAT, Time Clause, Enable, Log, Business Applications, Business Criticality, Business Partner, and Documentation. The rules are listed with their corresponding source and destination IP addresses, services, and associated applications like SAP ERP, CRM, RFP, HR system, SharePoint, Business Object, and L&D system.

ID	Name	Source	Destination	Service	Action	Source NAT	Destination NAT	Time Clause	Enable	Log	Business Applications	Business Criticality	Business Partner	Documentation
579277	FireFlow #781	g-usis_nrg_vip	g-usis-nrg_clients1	pm_sq_68638	✔	-	-	-	enabled	enabled	SAP ERP			
464157	FireFlow #782	g-usis_nrg_vip	g-usis-nrg_clients1	tcp-1812-1813-usisreply	✔	-	-	-	enabled	enabled	CRM			
832393	FireFlow #783	g-usis_nrg_vip	cos20001	snmp-162	✔	-	-	-	enabled	enabled	RFP			
500026	FireFlow #784	g-usis_nrg_vip	cos20001	g-usis-ports3	✔	-	-	-	enabled	enabled	HR system			
735626	FireFlow #785	h-10.176.47.7-usis1vip	g-vip	radius-1812-1813	✔	-	-	-	enabled	enabled	SharePoint			
188793	FireFlow #786	h-10.176.47.7-usis1vip	g-ggsn_oam	pm_sq_68638	✔	-	-	-	enabled	enabled	Business Object			
313855	FireFlow #787	h-10.176.47.7-usis1vip	g-ggsn_oam	udp-3799	✔	-	-	-	enabled	enabled	L&D system			
861062	FireFlow #789	h-10.176.47.7-usis1vip	g-ggsn_oam	tcp-1812-1813-usisreply	✔	-	-	-	enabled	enabled				
723244	FireFlow #790	h-10.176.47.1-nrg1appvip	g-ggsn_oam	pm_sq_68638	✔	-	-	-	enabled	enabled				
299010	FireFlow #791	h-10.176.47.1-nrg1appvip	g-ggsn_oam	udp-3799	✔	-	-	-	enabled	enabled				

Figure 1: AlgoSec associates each firewall rule with the relevant applications

Once you have this level of visibility, you can immediately see all active applications and their associated rules. All that's left to do is remove all of the redundant rules that are not associated with an active application. (Best practices recommend, however, that you do check usage reports before you delete these rules to ensure that active rules are not inadvertently deleted). While again, this can be done manually, a network security policy management solution such as AlgoSec, can automatically assist in the removal process while generating a full audit trail of the entire process.

Summary

There are many reasons why firewall rules become obsolete; from migrating applications/servers to a different datacenter, to the cloud or to decommissioning applications. Security best practices require that these firewall rulesets be reviewed and recertified from time to time. Rule recertification however, is never an easy task to perform and requires significant time and effort.

Taking an application-centric approach simplifies the process, especially when coupled with a solution that can handle much of the analysis and change management processes automatically. Taking this approach should be the standard way for maintaining ruleset hygiene and will deliver a tighter security posture and reduce risk, as well as save significant time and effort.

About AlgoSec

AlgoSec, a global cybersecurity leader, empowers organizations to secure application connectivity by automating connectivity flows and security policy, anywhere.

The AlgoSec platform enables the world's most complex organizations to gain visibility, reduce risk, achieve compliance at the application-level and process changes at zero-touch across the hybrid network.

Over 1,800 of the world's leading organizations trust AlgoSec to help secure their most critical workloads across public cloud, private cloud, containers, and on-premises networks.

