



Secure application connectivity.
Anywhere.



The firewall audit checklist: Six best practices for simplifying firewall compliance and risk mitigation

An AlgoSec Whitepaper

Ensuring continuous compliance

More regulations and standards relating to information security, such as the Payment Card Industry Data Security Standard (PCI-DSS), the General Data Protection Regulation (GDPR), Sarbanes-Oxley (SOX), Health Insurance Portability and Accountability Act (HIPAA), California Consumer Privacy Act (CCPA) and ISO 27001, have forced enterprises to put more emphasis—in terms of time and money—on compliance and the regular and ad hoc auditing of security policies and controls. While regulatory and internal audits cover a broad range of security checks, the firewall is featured prominently since it is the first and main line of defense between the public and the corporate network.

The number of enterprises that are not affected by regulations is shrinking. But even if you do not have to comply with specific government or industrial regulations and security standards, it is now commonplace to conduct regular, thorough audits of your firewalls. Not only do these audits ensure that your firewall configurations and rules meet the proper requirements of external regulations or internal security policy, but these audits can also play a critical role in reducing risk and actually improve firewall performance by optimizing the firewall rule base.

In today's complex, multi-vendor network environments, typically including tens or hundreds of firewalls running thousands of rules, completed a manual security audit now borders on the impossible. Conducting the audit process manually, firewall administrators must rely on their own experience and expertise—which can vary greatly across organizations—to determine if a given firewall rule should or should not be included in the configuration file. Furthermore, documentation of current rules and their evolution of changes is usually lacking. The time and resources required to find, organize and pour through all of the firewall rules to determine the level of compliance significantly impacts IT staff.

As networks grow in complexity, auditing becomes more cumbersome. Manual processes cannot keep up. Automating the firewall audit process is crucial as compliance must be continuous, not simply at a point in time.

The firewall audit process is arduous. Each new rule must pre-analyzed and simulated before it can be implemented. A full and accurate audit log of each change must be maintained. Today's security staffs now find that being audit-ready without automation is impractical if not virtually impossible.

It's time to look to automation along with the establishment of auditing best practices to maintain continuous compliance.

The Firewall audit checklist

Below, we share a proven checklist of six best practices for a firewall audits based on AlgoSec's extensive experience in consulting with some of the largest global organizations and auditors who deal with firewall audit, optimization and change management processes and procedures. While this is not an exhaustive list that every organization must follow, it provides guidance on some critical areas to cover when conducting a firewall audit.



Figure 1: Overview of the recommended firewall audit process

01 Gather key information prior to starting the audit

An audit has little chance of success without visibility into the business application connectivity within the network, including software, hardware, policies and risks. The following are examples of the key information required to plan the audit work:

- Copies of relevant security policies
- Access to firewall logs that can be analyzed against the firewall rule base to understand which rules are actually being used
- An accurate diagram of the current network and firewall topologies
- Reports and documents from previous audits, including firewall rules, objects and policy revisions
- Identification of all Internet Service Providers (ISP) and Virtual Private Networks (VPN)
- All relevant firewall vendor information including OS version, latest patches and default configuration
- Understanding all the business applications, key servers and information repositories in the network and the value of each

Once you have gathered this information, how are you going to aggregate it and storing it? Trying to track compliance on spreadsheets is a surefire way to make the audit process painful, tedious and time-consuming. Instead of spreadsheets, the auditor needs to document, store and consolidate this vital information in a way that enables collaboration with IT counterparts. With this convenience access, auditors you can start reviewing policies and procedures and tracking their effectiveness in terms of compliance, operational efficiency and risk mitigation.

02 Review the change management process

A good change management process is essential to ensure proper execution and traceability of firewall changes as well as for sustainability over time to ensure compliance continuously. Poor documentation of changes, including which business application is related to change, why each change is needed, who authorized the change, etc. and poor validation of the impact on the network of each change are two of the most common problems when it comes to change control.

- Review the procedures for rule-based change management. Just a few key questions to review include:
 - Are requested changes going through proper approvals?
 - What business applications will be impacted by the change?
 - Are changes being implemented by authorized personnel?
 - Are changes being tested?
 - Are changes being documented per regulatory and/or internal policy requirements? Each rule should have a comment that includes the change ID of the request and the name/initials of the person who implemented the change.
 - Is there an expiration date for the change?
- Determine if there is a formal and controlled process in place to request, review, approve and implement firewall changes. This process should include at least the following:
 - Business purpose for a change request
 - Duration (time period) for new/modified rule
 - Assessment of the potential risks associated with the new/modified rule
 - Formal approvals for new/modified rule
 - Assignment to proper administrator for implementation
 - Verification that change has been tested and implemented correctly
- Determine whether all of the changes have been authorized and flag unauthorized rule changes for further investigation.
- Determine if real-time monitoring of changes to a firewall are enabled and if access to rule-change notifications is granted to authorized requesters, administrators and stakeholders.

03 Audit the firewall's physical and OS security

It is important to be certain as to each firewall's physical and software security to protect against the most fundamental types of cyberattack.

- Ensure that firewall and management servers are physically secured with controlled access.
- Ensure that there is a current list of authorized personnel permitted to access the firewall server rooms.
- Verify that all appropriate vendor patches and updates have been applied.
- Ensure that the operating system passes common hardening checklists.
- Review the procedures used for device administration.

04 Clean up and re-certify rules

Removing firewall clutter and optimizing the rule base can greatly improve IT productivity and firewall performance.

- Identify which applications each rule serves and determine the usage of each application.
- Delete covered rules that are effectively useless.
- Delete or disable expired and unused rules and objects.
- Identify disabled, time-inactive and unused rules that are candidates for removal.
- Evaluate the order of firewall rules for effectiveness and performance.
- Remove unused connections, including source/destination/service routes, that are not in use.
- Detect similar rules that can be consolidated into a single rule.
- Identify overly permissive rules by analyzing the actual policy usage against firewall logs. Tune these rules as appropriate for policy and actual use scenarios.
- Analyze VPN parameters to identify unused users, unattached users, expired users, users about to expire, unused groups, unattached groups and expired groups.
- Enforce object-naming conventions.
- Document rules, objects and policy revisions for future reference.

05 Conduct a risk assessment and remediate issues

Essential for any firewall audit, a comprehensive risk assessment will identify risky rules and ensure that rules are compliant with internal policies and relevant standards and regulations.

- Identify potentially “risky” rules, based on industry standards and best practices, and prioritize them by severity. What is “risky” can be different for each organization depending on the network and the level of acceptable risk, but there are many frameworks and standards you can leverage that provide a good reference point. A few things to look for and validate include:
 - Are there firewall rules that violate your corporate security policy?
 - Are there any firewall rules with “ANY” in the source, destination, service/protocol, application or user fields, and with a permissive action?
 - Are there rules that allow risky services from your DMZ to your internal network?
 - Are there rules that allow risky services inbound from the Internet?
 - Are there rules that allow risky services outbound to the Internet?
 - Are there rules that allow direct traffic from the Internet to the internal network (not the DMZ)?
 - Are there any rules that allow traffic from the Internet to sensitive servers, networks, devices or databases?
- Analyze firewall rules and configurations against relevant regulatory and/or industry standards such as PCI-DSS, SOX, ISO 27001, NERC CIP, Basel-II, FISMA and J-SOX, as well as corporate policies that define baseline hardware and software configurations to which devices must adhere (See Figure 4 on page 8).
- Document and assign an action plan for remediation of risks and compliance exceptions found in risk analysis.
- Verify that remediation efforts and any rule changes have been completed correctly.
- Track and document that remediation efforts are completed.

06 Ongoing audits

Upon successful firewall and security device auditing, verifying secure configuration, proper steps must be put in place to ensure continuous compliance.

- Ensure that a process is established for continuous auditing of firewalls.
- Consider replacing error-prone manual tasks with automated analysis and reporting.
- Ensure that all audit procedures are properly documented, providing a complete audit trail of all firewall management activities.
- Make sure that a robust firewall-change workflow is in place to sustain compliance over time.
- This repeats Audit Checklist item #2 because it is necessary to ensure continuous compliance, i.e., compliance might be achieved now, but in a month, the organization might once again be out of compliance.
- Ensure that there is an alerting system in place for significant events or activities, such as changes in certain rules or the discovery of a new, high severity risk in the policy.

Automating firewall compliance audits with AlgoSec

When it comes to compliance, the firewall policy management solution must have the breadth and depth to automatically generate detailed reports for multiple regulations and standards. It also must support multiple firewalls and related security devices.

By combining this firewall audit checklist with the AlgoSec platform, organizations can significantly improve their security posture and reduce the pain of ensuring compliance with regulations, industry standards and corporate policies. Furthermore, they can ensure compliance continuously without spending significant resources wasting time and effort on complex security policies on a regular basis.

Let's go back through the checklist and look at a few examples of how AlgoSec can help.

Gain visibility of network policies and their changes

AlgoSec enables you to gather the key information needed to start the audit process. By generating a dynamic, interactive network map AlgoSec visualizes and helps you analyze complex networks. (See Figure 2.) You can view routing tables and effectively detect interfaces, subnets and zones. Additionally, AlgoSec provides you with visibility of all changes to your network security policies in real-time and creates detailed firewall audit reports to help approvers make informed decisions about changes that affect risk or compliance levels. Lastly, AlgoSec discovers all the business applications that run on your network and each of their associated connectivity flows.

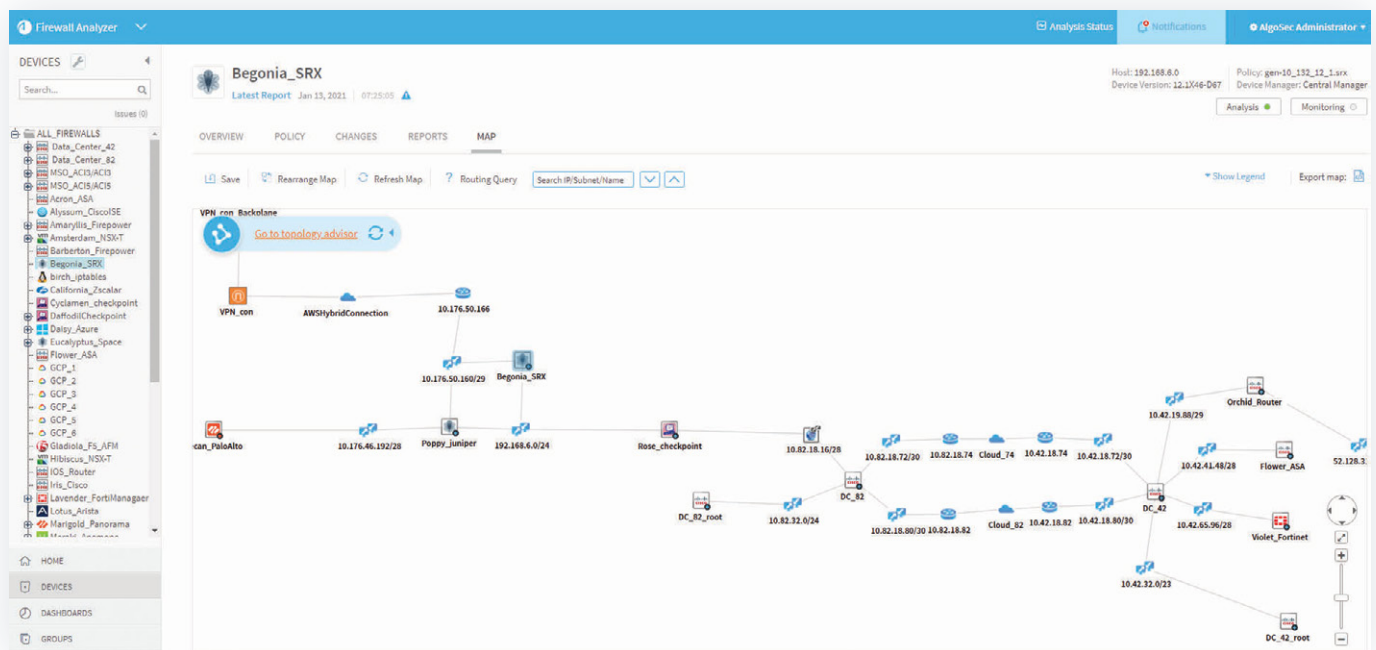


Figure 2: AlgoSec provides network topology awareness with a map that provides visibility of your firewalls and routers including the relevant interfaces, subnets and zones, and the ability to drill down to specific information about each device.



Understand the firewall changes in your network and automate the process

AlgoSec intelligently automates the security-policy change workflow, dramatically cutting the time required to process firewall changes, increasing accuracy and accountability, enforcing compliance and mitigating risk. In addition, AlgoSec provides flexible workflows and templates to help you manage change requests and tailor processes to your business needs.



Clean up, optimize and re-certify your existing firewall rules

AlgoSec enables you to optimize and clean up cluttered policies with actionable recommendations to:

- Consolidate similar rules.
- Recertify the applications instead of going through each rule in your policy
- Discover and remove unused rules and objects (See Figure 3).
- Identify and remove shadowed, duplicate, and expired rules.
- Reorder rules for optimal firewall performance while retaining policy logic.
- Tighten overly permissive rules based on actual usage patterns.

Not only does this help you improve the performance and extend the life of your firewalls, it also saves time when it comes to troubleshooting issues and IT audits. Plus, it creates a time savings during rule recertification, as each application is associated with multiple connectivity needs requiring multiple firewall rules.

	ID	FROM	TO	SOURCE	DESTINATION	SERVICES	ACTION	COMMENT	LOG	SCHEDULE	Business Applications	Business Criticality	Business Partner	Documentation
VPNclient -> port16 (1)														
<input type="checkbox"/>	11	VPNclient	port16	all	all	ICMP_ANY	ACCEPT	FireFlow #401] allow plings	<input type="checkbox"/>	always				
Zone_VPN_carrot -> port16 (1)														
<input type="checkbox"/>	10	Zone_VPN_carrot	port16	carrot.int	violet_int_10-8 violet_int_old	HTTP HTTPS DNS RDP ICMP_ANY	ACCEPT		<input checked="" type="checkbox"/>	always				
Zone_VPN_onion -> port16 (1)														
<input type="checkbox"/>	8	Zone_VPN_onion	port16	onion.int	violet_int_10-8 violet_int_old	HTTP HTTPS DNS RDP	ACCEPT		<input checked="" type="checkbox"/>	always				
Zone_VPN_tomato -> port16 (1)														
<input type="checkbox"/>	4	Zone_VPN_tomato	port16	debby_int	dogs_support violet_int_10-8 violet_int_old	HTTP ICMP_ANY	ACCEPT		<input checked="" type="checkbox"/>	always				
port1 -> port16 (4)														
<input type="checkbox"/>	13	port1	port16	all	violet_int_10-8	ANY	SSL-VPN		<input checked="" type="checkbox"/>					FireFlow #412]

Figure 3: Unused rules that AlgoSec has identified for removal.



Conduct a risk assessment and remediate issues

AlgoSec enables you to effectively discover and prioritize all risks and potentially risky rules in the firewall policy, leveraging the largest risk knowledgebase available. The knowledgebase includes industry regulations, best practices, customizable corporate security policies and scanner-based vulnerability information. AlgoSec assigns and tracks a security rating for each device and group of devices to help you to quickly pinpoint devices that require attention and to measure the effectiveness of a security policy over time.

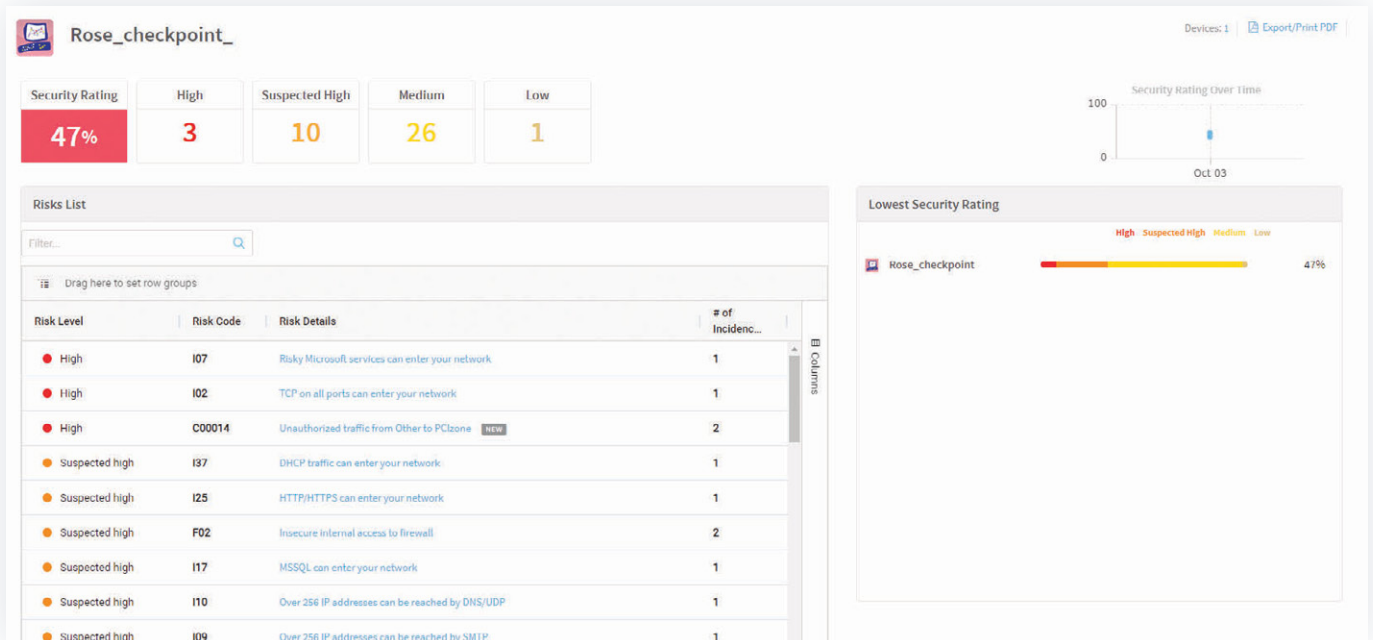


Figure 4: AlgoSec identifies and prioritizes risky rules based on industry standards and frameworks and provides detailed information of source, destination, service, as well as user and application when analyzing next-generation firewalls.



Out-of-the-box compliance reports

AlgoSec ensures continuous compliance and provides you with an in-depth view of your firewall compliance status by automatically generating reports for industry regulations, including Payment Card Industry Data Security Standard (PCI DSS), GDPR, Sarbanes-Oxley (SOX), Financial Instruments and Exchange Act (J-SOX, also known as Japan-SOX), North American Electric Reliability Corporation Critical Infrastructure Protection (NERC CIP), and International Organization for Standardization (ISO 20071). If the network security policy doesn't adhere to regulatory or corporate standards, the reports identify the exact rules and devices that cause gaps in compliance. A single report provides visibility into risk and compliance associated with a group of devices.


PCI DSS Requirements	AlgoSec Feature	Setting	Details	Status
1.1 Establish firewall configuration standards that include the following:				
1.1.1 A formal process for approving and testing all network connections and changes to the firewall and router configuration	Change Management	On	The AlgoSec FireFlow product performs a "what-if" risk check on every change request (prior to implementation). To learn more about AlgoSec FireFlow please visit the AlgoSec web site , or contact your AlgoSec representative. AlgoSec FireFlow is licensed in your environment.	✓
	ActiveChange	On	The AlgoSec ActiveChange technology can be used in order to changes firewall configuration. AlgoSec ActiveChange feature is licensed in your environment.	✓
	Change History	On	Records available since 2023-07-31	✓
	E-Mail Notification	On	These users get an email when the following occurs: AlgoSec Administrator - Report is ready, Real time alerting Sue Security - Report is ready, Real time alerting algototalgosec - Report is ready, Real time alerting Ned NetOps - Report is ready, Real time alerting	✓
1.1.2a Examine diagram(s) and observe network configurations to verify that a current network diagram exists and that it documents all connections to cardholder data, including any wireless networks.	Connectivity Diagram	On	The connectivity diagrams are current as of 2023-10-03 : Rose_checkpoint 	✓
1.1.3 Current diagram that shows all cardholder data flows across systems and networks.	Network Map	On	The Network Map tab on AlgoSec web interface homepage allows running a routing query to trace problems of traffic traveling from and to specific IP addresses.	✓
	AppViz Application Diagram	On	The AlgoSec AppViz product includes a visual representation of every applications' flows in an Application Diagram. To learn more about AlgoSec AppViz please visit the AlgoSec web site , or contact your AlgoSec representative. AlgoSec AppViz is licensed in your environment.	✓
1.1.4a Examine the firewall configuration standards and verify that they include	-	-	Verify that firewall configuration standards include this requirement	•

Figure 5: PCI DSS firewall compliance report automatically generated by AlgoSec.

Conclusion

Ensuring and proving compliance typically require significant organizational resources and budget. With the growing litany of regulations, the cost and time involved in the audit process is increasing rapidly. Armed with the firewall audit checklist and the AlgoSec platform you can:

Reduce the time required for an audit — Manual reviews can take a significant amount of time to produce a report for each firewall in the network. AlgoSec aggregates data across a defined group of firewalls and devices for a unified compliance view, doing away with running reports for each device, thereby saving a tremendous amount of time and effort that is wasted on collating individual device reports. AlgoSec enables you to produce a report in minutes, reducing time and effort by as much as 80%.

Improve compliance while reducing costs — As the auditor's time to gather pertinent information and analyze the network security status is reduced, the total cost of the audit decreases substantially. AlgoSec facilitates the remediation of non-compliant items by providing actionable information that further reduces the time to re-establish a compliant state.

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.

