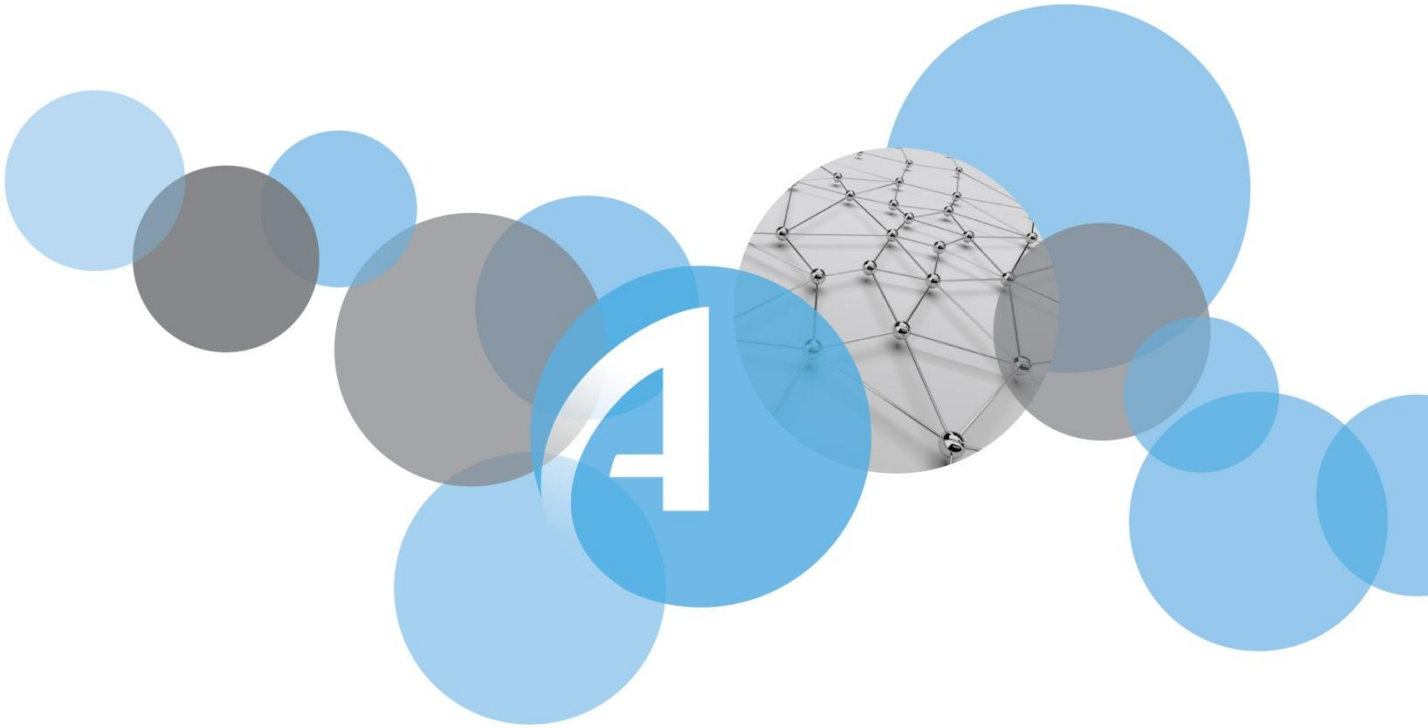


The Firewall Audit Checklist

Six Best Practices for Simplifying Firewall Compliance and Risk Mitigation

The Need to Ensure Continuous Compliance

Regulations and standards relating to information security such as the Payment Card Industry Data Security Standard (PCI-DSS), Sarbanes-Oxley, ISO 27002, the Critical Infrastructure Information Act of 2002 and others has put more emphasis on compliance and the regular 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 line of defense between the public and the corporate network.

Even if you do not have to comply with specific government or organizational standards, it is now commonplace — and nearly mandatory — that you conduct regular, thorough audits of your firewalls. This not only helps ensure that your firewall configuration meets the correct criteria for an external standard or internal security policy, but a firewall audit can also play an important role to reduce overall risk factors and actually improve firewall performance by its inclusion of certain tasks such as optimizing your firewall rule base.

In today's complex, multi-vendor network environments, which typically include thousands of firewall rules, the ability to complete a manual audit of your firewall has become as Forrester Research puts it "nearly impossible[1]". When this process is conducted manually, the firewall administrator has to rely on his own experience and expertise — which can vary greatly across organizations — to determine if a firewall rule should or should not be included in the configuration file. Furthermore, if performed manually, documentation of rules and/or rule changes is usually lacking. The time and resources required to pour through all of the firewall rules and determine compliance/non-compliance significantly impacts IT staff.

Automating the firewall audit process is crucial as compliance must be continuous, not simply a point in time. Firewall audits require that each new rule is pre-analyzed and simulated prior to being implemented, and that a full audit log of the change is created. Addressing this type of compliance requirement without sound processes and automated solutions is extremely difficult.

The Firewall Audit Checklist

The following is a checklist of six best practices for a firewall audit based on AlgoSec's experience in consulting with some of the largest global organizations and auditors on firewall audit, optimization and change management procedures. This should not be viewed as an exhaustive list, but it does provide guidance on some critical areas to have covered when conducting a firewall audit.

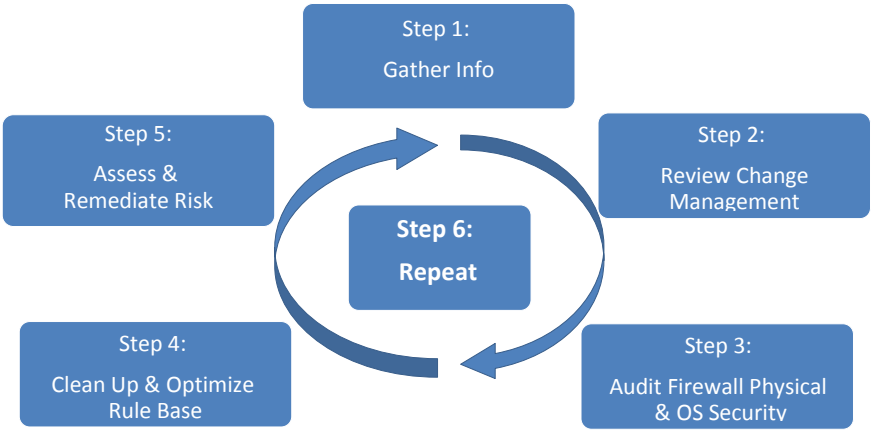


Figure 1: Overview of the Recommended Firewall Audit Process

[1] Forrester Research, Market Overview: Firewall Auditing Tools, 2009

1. Gather Key Information Prior to Starting the Audit

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

a. Obtain copies of relevant security policies.

b. Obtain access to firewall logs that can be analyzed against the firewall rule base to understand what is actually being used.

c. Obtain a diagram of the current network and firewall topologies.

d. Obtain reports and documents of previous audits, including firewall rules, objects and policy revisions.

e. Identify all Internet Service Providers (ISP) and Virtual Private Networks (VPN).

f. Obtain all relevant firewall vendor information including OS version, latest patches and default configuration.

g. Understand all the key servers and key information repositories in the network and their relative values to the company.

Once you have gathered this information, how are you aggregating it and storing it? Spreadsheet compliance is a surefire way to make the audit process painful. Document, store and consolidate this important information in a way that enables collaboration with your IT counterparts. Then you can start reviewing policies and procedures and tracking their effectiveness in terms of compliance, operational efficiency and risk mitigation.

2. Review Your Change Management Process

A good change management process is essential to ensure proper execution and traceability of firewall changes, as well as sustainability over time to ensure continuous compliance vs. point-in-time compliance. Poor documentation of changes, including why the change is needed, who authorized the change, etc. and poor validation of the impact on the network are two of the most common issues when it comes to change control.

a. Review the procedures for rule-base maintenance. Just a few key questions to review include:

- Are requested changes going through proper approvals?
- Are changes being implemented by authorized personnel? And are they being tested?
- Are the changes being documented per regulatory 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?

b. Determine if there is a formal and controlled process in place to request, review, approve and implement firewall changes.

Note: This process should include at least the following:

a) Business purpose for the request
b) Duration (time period) for the new/modified rule

c) Assessment of the potential risks associated with the new/modified rule
d) Formal approvals for the new/modified rule
e) Assignment to proper administrator for implementation
f) Verification that change has been tested and implemented correctly

c. Determine whether or not all of the changes been authorized, and flag any unauthorized rule changes for further investigation.

d. Determine if real-time monitoring of changes to the firewall is enabled and access to rule change notifications is granted to authorized requestors, administrators and stakeholders.

3. Audit the Firewall Physical and OS Security

This is important to help protect against the most fundamental types of attack. If you define corporate baselines and report against them, you can be assured of always knowing the configuration status and how your firewalls stack up to policy.

a. Ensure firewall and management servers are physically secured with controlled access.

b. Ensure there is a current list of authorized personnel permitted to access the firewall server rooms.

c. Verify that all appropriate vendor patches and updates have been applied.

d. Ensure the operating system passes common hardening checklists.

e. Review the procedures used for device administration.

4. Cleanup and Optimize Your Rule Base

Removing firewall clutter and optimizing the rule base can greatly improve IT productivity and firewall performance. Additionally, optimizing firewall rules can significantly reduce a lot of unnecessary overhead in the audit process.

a. Delete covered rules that are effectively useless.

b. Delete or disable expired and unused rules and objects.

c. Identify disabled, time inactive and unused rules which are candidates for removal.

d. Evaluate the order of firewall rules for effectiveness/performance.

e. Remove unused connections, including specific source/destination/service routes that are not in use.

f. Detect similar rules that can be consolidated into a single rule.

g. Identify overly permissive rules by analyzing the actual policy usage against the firewall logs. Tune these rules as appropriate for policy and actual real use scenarios. For example, “ANY” might be used for the source address in several rules when actual traffic only originates from a handful of IP addresses.

h. Analyze VPN parameters to identify unused users, unattached users, expired users, users about to expire, unused groups, unattached groups and expired groups.

i. Enforce object naming conventions.

j. Document rules, objects and policy revisions for future reference.

5. 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.

a. Identify any and all 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?

b. 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 below.

c. Document and assign an action plan for remediation of risks and compliance exceptions found in risk analysis.

d. Track and document that remediation efforts are completed.

e. Verify that remediation efforts and any rule changes have been completed correctly.

6. Ongoing Audits

Now that you have successfully audited your firewall and secured its configuration, you need to ensure the proper steps are in place to ensure continuous compliance.

a. Ensure a process is established for continuous auditing of firewalls.

b. Consider replacing error-prone manual tasks with automated analysis and reporting.

c. Ensure all audit procedures are properly documented, providing a complete audit trail of all firewall management activities.

d. Make sure that solid firewall change workflow is in place to sustain compliance over time.

Note: This is purposely repetitive from Audit Checklist item #2 because without change management, you won't be able to ensure continuous compliance – you will go through the cleanup and optimization at a point in time, but a month later you may no longer be compliant.

e. Ensure 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, you want to ensure that your firewall policy management solution has the breadth and depth to automatically generate detailed reports for multiple regulations and standards, and support multiple firewalls and related security devices.

By combining this firewall audit checklist with a solution such as the AlgoSec Security Management Suite, and you can significantly improve your security posture and reduce the pain of ensuring compliance with regulations, industry standards and corporate policies. Furthermore, you can ensure continuous compliance – without spending significant resources pouring through 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 and Changes to Your Network Policies

AlgoSec Security Management Suite enables you to gather all of the key information you need to be able to start the audit process. AlgoSec generates a dynamic, interactive network map to help visualize and analyze complex networks as seen below in Figure 2 – you can view routing tables and automatically detect all interfaces, subnets and zones. Additionally, AlgoSec provides you with visibility of all changes to your network security policy in real-time and creates detailed firewall audit reports to help approvers make informed decisions about changes that affect risk or compliance levels.

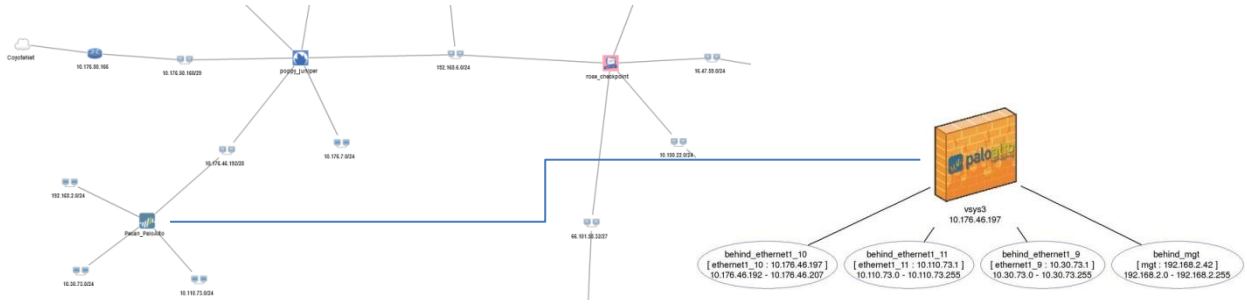


Figure 2: AlgoSec provides network topology awareness and a topology map provides visibility of all firewalls and routers including all relevant interfaces, subnets and zones, with the ability to drill down to specific information about each device.

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. AlgoSec Security Management Suite provides flexible workflows and templates to help you better manage change requests and tailor processes to your specific business needs (see Figure 3).

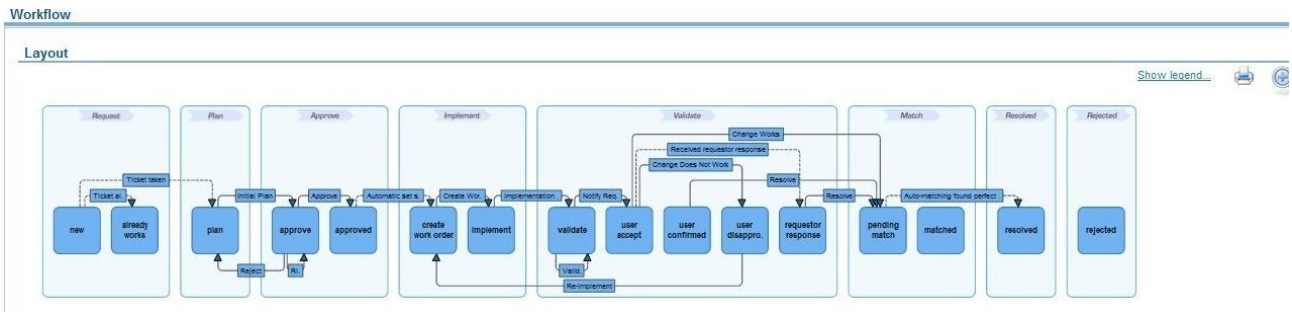


Figure 3: AlgoSec FireFlow's visual workflow editor allows you to customize the change workflow to fit your specific requirements.

Clean Up and Optimize Your Rule Base

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

- consolidate similar rules
- discover and remove unused rules and objects (see figure 4)
- 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.

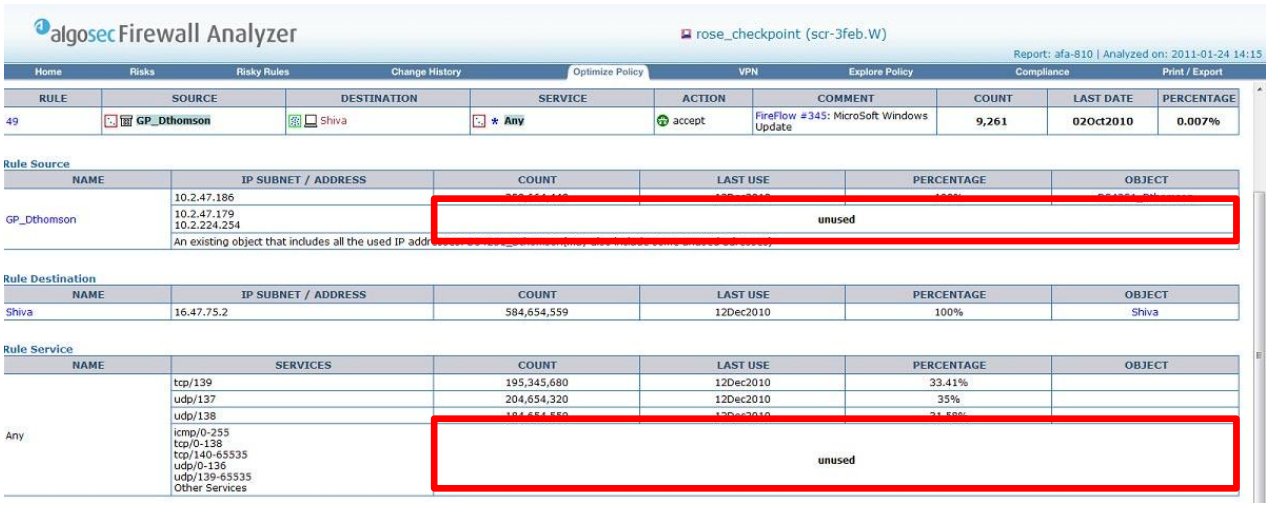
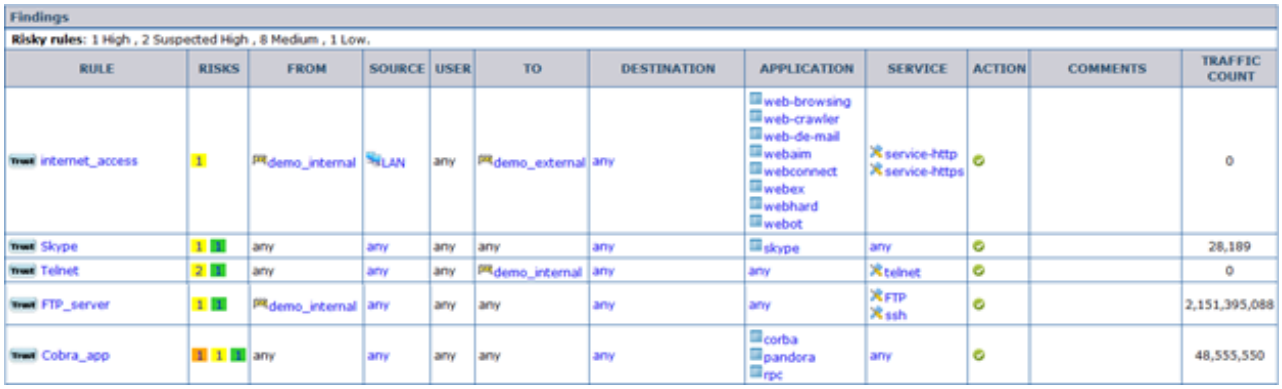


Figure 4: This example shows unused rules that AlgoSec has identified for removal.

Conduct a Risk Assessment and Remediate Issues

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



Findings

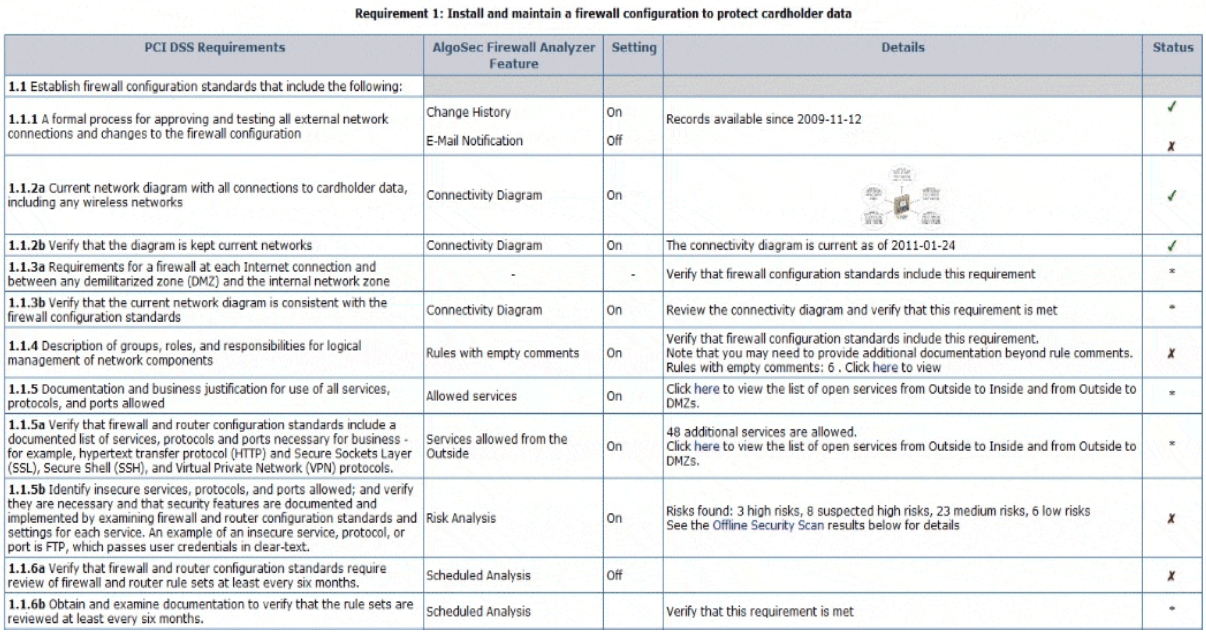
Risky rules: 1 High , 2 Suspected High , 8 Medium , 1 Low.

RULE	RISKS	FROM	SOURCE	USER	TO	DESTINATION	APPLICATION	SERVICE	ACTION	COMMENTS	TRAFFIC COUNT
Trust internet_access	1	demo_internal	LAN	any	demo_external	any	web-browsing web-crawler web-de-mail webaim webconnect webex webhard webot	service-http service-https	✓		0
Trust Skype	1 1	any	any	any	any	any	skype	any	✓		28,189
Trust Telnet	2 1	any	any	any	demo_internal	any	any	telnet	✓		0
Trust FTP_server	1 1	demo_internal	any	any	any	any	any	FTP ssh	✓		2,151,395,088
Trust Cobra_app	1 1 1	any	any	any	any	any	corba pandora rpc	any	✓		48,555,550

Figure 5: 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 Security Management Suite ensures continuous compliance and instantly provides you with a view of your firewall compliance status by automatically generating reports for industry regulations, including PCI-DSS (Payment Card Industry Data Security Standard), SOX (Sarbanes-Oxley), J-SOX (Financial Instruments and Exchange Act, also known as “Japan-SOX), NERC CIP (North American Electric Reliability Corporation Critical Infrastructure Protection), and ISO-27001 (International Organization for Standardization). 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 (see figure 6).



Requirement 1: Install and maintain a firewall configuration to protect cardholder data

PCI DSS Requirements	AlgoSec Firewall Analyzer 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 external network connections and changes to the firewall configuration	Change History E-Mail Notification	On Off	Records available since 2009-11-12	✓ ✗
1.1.2a Current network diagram with all connections to cardholder data, including any wireless networks	Connectivity Diagram	On		✓
1.1.2b Verify that the diagram is kept current networks	Connectivity Diagram	On	The connectivity diagram is current as of 2011-01-24	✓
1.1.3a Requirements for a firewall at each Internet connection and between any demilitarized zone (DMZ) and the internal network zone	-	-	Verify that firewall configuration standards include this requirement	*
1.1.3b Verify that the current network diagram is consistent with the firewall configuration standards	Connectivity Diagram	On	Review the connectivity diagram and verify that this requirement is met	*
1.1.4 Description of groups, roles, and responsibilities for logical management of network components	Rules with empty comments	On	Verify that firewall configuration standards include this requirement. Note that you may need to provide additional documentation beyond rule comments. Rules with empty comments: 6 . Click here to view	✗
1.1.5 Documentation and business justification for use of all services, protocols, and ports allowed	Allowed services	On	Click here to view the list of open services from Outside to Inside and from Outside to DMZs.	*
1.1.5a Verify that firewall and router configuration standards include a documented list of services, protocols and ports necessary for business - for example, hypertext transfer protocol (HTTP) and Secure Sockets Layer (SSL), Secure Shell (SSH), and Virtual Private Network (VPN) protocols.	Services allowed from the Outside	On	48 additional services are allowed. Click here to view the list of open services from Outside to Inside and from Outside to DMZs.	*
1.1.5b Identify insecure services, protocols, and ports allowed; and verify they are necessary and that security features are documented and implemented by examining firewall and router configuration standards and settings for each service. An example of an insecure service, protocol, or port is FTP, which passes user credentials in clear-text.	Risk Analysis	On	Risks found: 3 high risks, 8 suspected high risks, 23 medium risks, 6 low risks See the Offline Security Scan results below for details	✗
1.1.6a Verify that firewall and router configuration standards require review of firewall and router rule sets at least every six months.	Scheduled Analysis	Off		✗
1.1.6b Obtain and examine documentation to verify that the rule sets are reviewed at least every six months.	Scheduled Analysis		Verify that this requirement is met	*

Figure 6: Example of a PCI DSS firewall compliance report automatically generated by AlgoSec Firewall Analyzer.

Conclusion

Ensuring compliance and being able to prove it typically requires significant organizational resources and budget. Armed with the firewall audit checklist and with a firewall policy management solution such as AlgoSec, you can:

Reduce the time required to undergo 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 single compliance view, instead of running reports for each individual device, saving a tremendous amount of time and effort that may be wasted on collating individual device reports. AlgoSec enables you to produce a report in minutes, reducing time by as much as 80%.

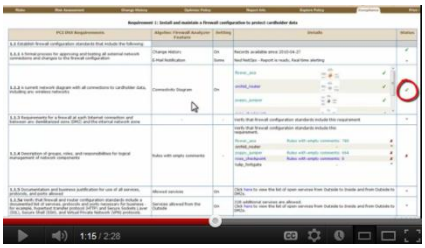
> ***"The total process used to take three months. Now we can get in a click of a button what took two to three weeks per firewall to produce manually."***
>
> **Marc Silver, Discovery SA**

Reduce the cost of compliance

As the auditor's time to gather pertinent information and analyze the network security status is reduced, the audit cost decreases substantially. Additionally, AlgoSec facilitates the remediation of non-compliant items by providing actionable information, reducing the time to regain a compliant state and thus saving costs.

Next Steps

- **Watch a brief demo** - to see how you can automatically generate compliance reports with AlgoSec Security Management Suite



- **Evaluate the AlgoSec Security Management Suite**

About AlgoSec

AlgoSec is the market leader in network security policy management. AlgoSec enables security and operations teams to intelligently automate the policy management of firewalls, routers, VPNs, proxies and related security devices, improving operational efficiency, ensuring compliance and reducing risk.

More than 800 of the world's leading enterprises, MSSPs, auditors and consultancies rely on AlgoSec Security Management Suite for unmatched automation of firewall operations, auditing and compliance, risk analysis and the security change workflow.

AlgoSec is committed to the success of every single customer, and offers the industry's only money-back guarantee. For more information, visit www.AlgoSec.com.

300 Colonial Center Parkway
Suite 100
Roswell, GA 30076
USA

T: +1-888-358-3696
F: +1-866-673-7873
E: info@algosec.com

AlgoSec.com