FIREMON

IMPROVE SECURITY OUTCOMES. IMPROVE SECURITY OUTCOMES.

Compliance Audit Preparation Guide

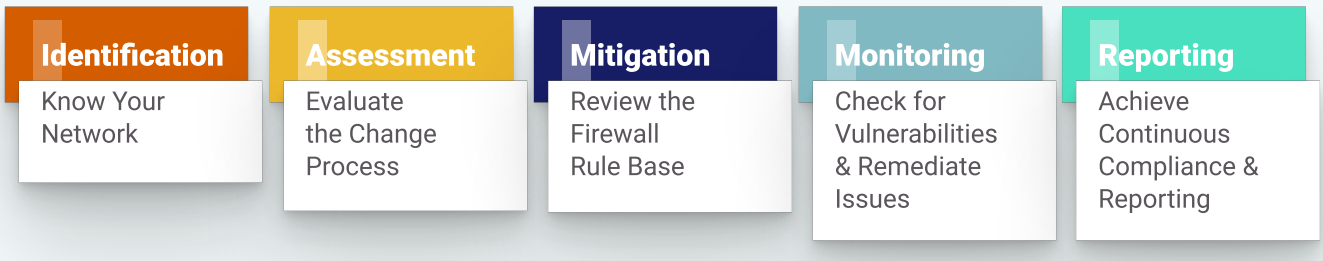
INTRODUCTION

Security compliance audits are getting a lot of coverage these days thanks to standards such as SOX, PCI-DSS, and HIPAA. If a specific compliance standard isn't on your radar, business relationships with partners or customers may require you to still prove that your network is secure.

Beyond compliance requirements, the firewall audit is a security best practice and an important mechanism for understanding your current security position. Firewall audits increase your chances of catching weaknesses and finding blind spots and dark zones where your policies need to adapt. They also help prove you have been doing your due diligence – often, an audit finding helps correct policies and procedures that are incorrectly documented or omitted. Using documentation to demonstrate that you review your security controls regularly is critical to addressing a lawsuit, breach, or regulatory issue that calls your security standards into question. Of course, preventing these issues is even better.

5 Key Steps

to Prepare for Your Firewall Audit



Identification Know Your Network

Knowing what you have in your environment is the cornerstone of your security practice and, ultimately, the success of your audit. Large, complex enterprises understandably struggle with managing complex, fast-changing environments – what you don't know *can* hurt you. Dark zones and blind spots in your network only serve to give an auditor reason to question your security posture.

The problem of unauthorized, rogue, and insecure connections between the enterprise and the Internet continues to plague network and security managers alike. Disparate security management tools for cloud and physical networks limit the visibility of shadow networks and cloud instances that may harbor unknown threats. These backdoors provide a method by which the transport of critical data can circumvent security controls and escape the network.

Ask Yourself These Questions to Ensure That You Know Every Part of Your Network Environment:

- What is your presumed list of endpoints/ network devices?
- Can you demonstrate that your asset management is robust and up to date?
- How do you discover additional or new devices added to the network?
- Can you detect unauthorized forwarding devices (Layer2/Layer3)?
- Are there unknown or non-responding networks in your environment?
- Have you identified any paths that may leak data around your security controls?
- If you must supply credentials to your network devices, are these credentials ocumented? Are they rotated regularly?
- Have you identified and documented all zones that keep sensitive data per regulatory equirements?
- Do you have a complete document of "Network Source of Truth" and topology map?

HOW FIREMON CAN HELP

FireMon provides real-time visibility, vulnerability, and risk management that enables cloud, network, and security teams to find and secure unknown, rogue and shadow clouds, network infrastructure, and endpoints.

FIREMON HELPS YOU DISCOVER MORE BY:

- **Eliminating 100% of your blind spots** and monitor changes or unusual behaviors to eliminate any gaps in coverage that may leave you exposed.
- **Discovering, maps, and alerts** on topology changes across the entire hybrid enterprise, including multi-cloud environments.
- **Monitoring the hybrid infrastructure** for telltale signs of nefarious activity and prioritizes findings for investigation and remediation.
- **Finding inbound and outbound leak paths** to the Internet, virtual private cloud, in between network segments, firewalled enclaves, or across IT/OT environments

Assessment Evaluate the Change 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. 83% of all unplanned network outages are caused by mistakes made during an approved change; 70% of these mistakes are firewall related.

The goal of this step is to make sure that requested changes were adequately approved, implemented, and documented.

The Basic Questions You Should Be Asking When You Audit a Firewall Change Are:

- Is the requester documented, and is s/he authorized to make firewall change requests?
- Is the business reason for the change documented?
- Are there proper reviewers and approval signatures (electronic or physical)?
- Were the approvals recorded before the change was implemented?
- Are the approvers all authorized to approve firewall changes (you will need to ask for a list of authorized individuals)?
- Are the requested changes well documented in the change ticket?
- Has there been an assessment of the potential risks associated with the new/modified rule?
- Is there documentation of the change window and install date for each change?
- Is there an expiration date for the change?
- Is there verification and documentation that changes were tested and implemented correctly?
- Are you monitoring firewall updates in real time to verify execution?

HOW FIREMON CAN HELP

FireMon Automation delivers a comprehensive blueprint for security process automation that accelerates and streamlines policy management and intelligently upgrades your approval workflows.

FIREMON HELPS YOU DISCOVER MORE BY:

- **Integrating with your existing ticketing systems** to enable new requests to filter directly into our change automation platform and customizing request forms to ensure all relevant change information is captured up front.
- **Delivering a comprehensive set of security policy automation capabilities** that drive smart security process automation to effectively address your unique use cases, infrastructure, or compliance requirements.
- **Providing insight into any requests** that would create duplicate rules, as well as any rules that allow similar access to a new request. These efforts work to reduce complexity and increase the efficiency of your hybrid network.
- **Performing a pre-change impact analysis** that simulates a potential rule change and analyzes its impact on compliance and security.

Mitigation **Review the Firewall Rule Base**

The next logical step is usually a review of the firewall rule base or policies. The methodology for this step varies widely among auditors because it has traditionally been challenging to do and heavily technology dependent.

Ask Yourself:

- How many rules does the policy have? How many did it have at the last audit? Last year?
- Are there any undocumented rules?
- Are there any redundant rules that should be removed?
- Are there any rules that are no longer used?
- Are there any services in the rules that are no longer used?
- Are there any groups or networks in the rules that are no longer used?
- Are there any firewall rules with ANY in three critical fields (source, destination, service/ protocol) and a permissive action?
- Are there any overly permissive rules: rules with more than 1000 IP addresses allowed in the source or destination?
- Are there any rules that violate your corporate security policy?
- Are there any rules that allow risky services inbound from the Internet? E.g., protocols that pass login credentials in the clear like telnet, ftp, pop, imap, http, netbios, etc.
- Are there any rules that allow risky services outbound to the Internet?
- Are there any 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?

FIREMON HELPS YOU WITH SECURITY ASSESSMENTS AND RULE CLEAN UP BY:

- **Eliminating duplicate or shadowed rules** that adversely impact the performance of your devices and introduce unnecessary complexity to your network.
- **Performing real-time analysis** and providing an extensive history for rule and object usage in a policy to help you easily identify unused rules to optimize your network devices for peak performance and reduce risk.
- **Showing unique traffic patterns t**hat exist in a rule and report on what data is flowing across a broadly defined address range.
- **Automating event-driven reviews** and verification, recertifying the rules and decommissioning those that are not needed.

Monitoring | Check for Vulnerabilities & Remediate Issues

Essential for any firewall audit, a comprehensive risk assessment will identify risky rules, paths, and connections.

What is “risky” can be different for each organization depending on the network and the level of acceptable risk. The best way to combat unwarranted access is to identify and analyze areas of vulnerability preemptively. However, the complex nature of security policies combined with the time-consuming burden of patching tens of thousands of vulnerabilities makes threats challenging to see and assess.

Vulnerability Points to Check:

- Check the network for published vulnerabilities is software, hardware, and network devices
- 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

FIREMON HELPS YOU MANAGE RISK BY:

- **Scoring all attack simulations** for risk and impact and then re-score once you’ve made improvements to determine the impact changes.
- **Tracing possible paths** that attackers might use to gain access to your critical assets.
- **Integrating with your vulnerability management solutions** (Qualys, Rapid7, and Tenable) to measure risk and identify potential attack penetration in your network.
- **Detecting in real-time** when new access will uncover vulnerable systems, scope proposed changes before implementation and streamline the approval process for access requests that have little impact to your risk profile

Reporting Achieve Continuous Compliance & Reporting

Once firewall and security device auditing are complete, and a secure configuration has been applied to all devices, proper steps must be put in place to ensure continuous compliance.

Ask Yourself:

- Do you have a process to ensure on-going firewall audits?
- Consider replacing error-prone manual tasks with automated analysis and reporting Ensure that all procedures are adequately 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 Repeat Audit Checklist item, Auditing the Change, Process to ensure continuous compliance, i.e., compliance might be achieved now, but in a month, the organization may have drifted out of compliance
- Ensure that there is an alerting system in place for significant events or activities, such as changes in specific rules or the discovery of a new, high severity risks

FIREMON HELPS YOU MANAGE RISK BY:

- **Providing out-of-the-box and customizable assessments** to help you ensure compliance with regulatory bodies or internal best practices. Outof-the-box reporting includes the most common compliance standards, including those based on PCI-DSS, NERC-CIP, GDPR, and others. Our customization engine ensures that the assessments and reports are tailor-made for your needs.
- **Automatically identifying rules** that require immediate analysis based on real-world events. Event-driven rules are analyzed on criteria including time-frame expiration, critical security control failure, periodic review, or ad-hoc query to determine the appropriate remediation.
- **Providing documentation of rule certification decisions** and justification to aid in compliance audits. You can review detailed information regarding each discussed rule with the option to approve or reject current rule configurations

Achieve Continuous Compliance with FireMon

Highly-customizable reports deliver a one-click overview of compliance throughout the entire environment tailored to precise business needs. Automatic scans identify and remove rules that violate internal and external compliance standards including PCI-DSS, HIIPA, and GDPR. Real-time detection identifies and notifies administrators on existing policy violations and scans for any new ones before changes are deployed.

FireMon supports the latest firewall and policy enforcement technologies spanning the data center to the cloud.

Combining the industry's broadest support for firewalls, devices, and cloud security groups with flexible architecture and the most robust API on the market, FireMon delivers complete visibility and control across the entire IT landscape to automate policy changes, compliance, and minimize policy-related risk.

Since creating the first-ever security policy management solution in 2001, FireMon has remained at the forefront of the security management category, delivering industry-first functionality such as firewall behavior testing, workflow integration, traffic flow analysis, and rule recertification. Over 1,700 customers around the world trust FireMon to gain visibility into and secure their networks.

ALWAYS BE COMPLIANT

SCHEDULE DEMO

SG0099-EN-20200101-1

FIREMON