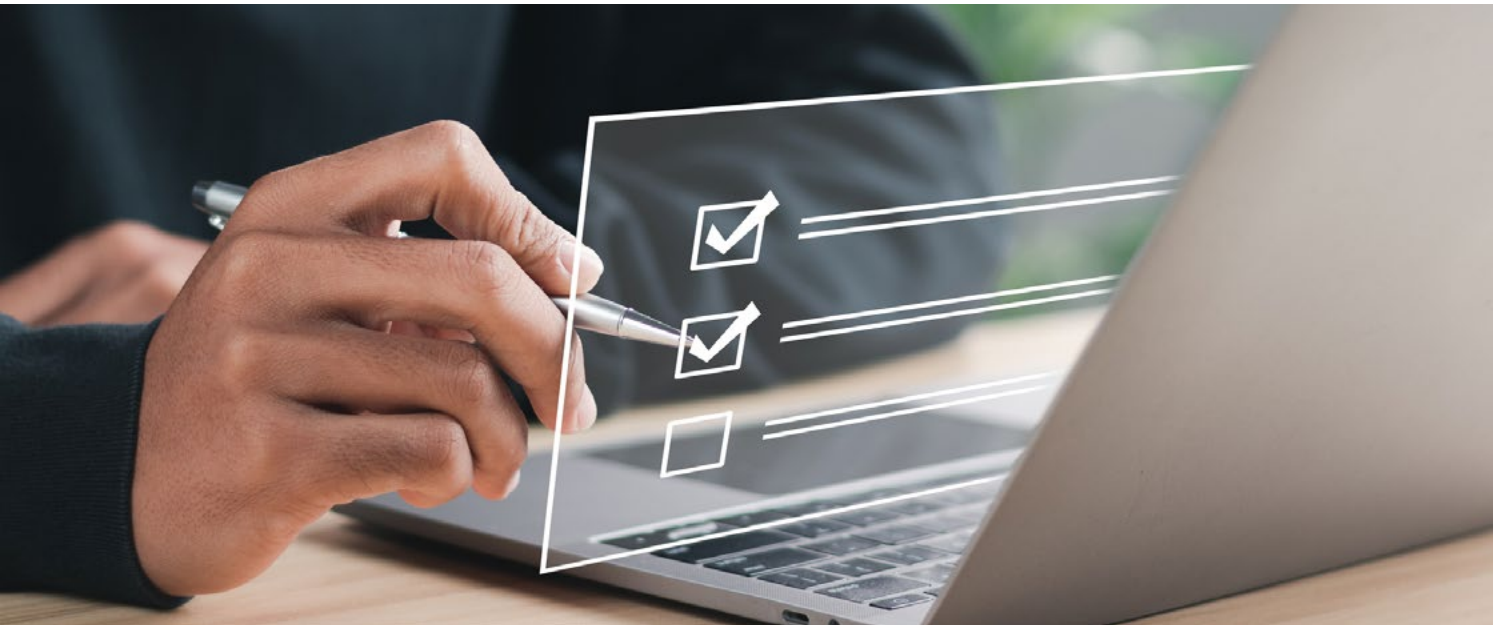
tufin
The Security Policy Company.

# Firewall Audit Checklist

Industry standards such as SOX, PCI-DSS 4.0, and HIPAA have shaped and informed the way organizations perform security audits. Even if immediate compliance with these standards isn't mandatory and is optional for your organization, maintaining secure business relationships with partners or customers is necessary in demonstrating the integrity of your network.

Different from network audits, which provide a broad evaluation of an organization's entire network infrastructure, a firewall audit focuses on the specific security measures the firewall initiates to protect the network from unauthorized access and potential threats.

Use this guide to determine if you're up to speed on firewall management best practices and learn how to meet compliance, reduce audit fines, and better secure your network.



## Step 1: Firewall Audit Overview

In addition to meeting compliance, conducting firewall audits is considered the gold standard since firewall audits enhance the likelihood of identifying vulnerabilities in your network security stance and pinpoint areas where policy adjustments are required.

Beyond the proactive approach to compliance, firewall audits are crucial to demonstrating due diligence in assessing security controls and policy measures.

Here are the steps involved in a typical audit process:

1. Review your firewall security policy
2. Review your firewall operations policies
3. Review who's authorized to make changes
4. Review your firewall change procedures
5. Review the firewall system design
6. Review the firewall review process

Let's delve into each below. Use the questions under each section as a guide to determine if you meet compliance within each subcategory.

**1. Review Your Firewall Security Policy.**

Before conducting an audit, you must understand the specific criteria you are investigating. Your organization should possess a documented set of security guidelines outlining policies for firewalls and associated security infrastructure. Additionally, if compliance with industry, government, or regulatory standards is a requirement, it is crucial to review those standards and ensure alignment with your corporate security guidelines.

**2. Review Your Firewall Operations Policies.**

Every organization needs well-defined protocols for addressing incidents related to firewall security that encompasses the following:

- Details of the escalation procedure
- Specifies authorized responders
- Outlines coordination processes with law enforcement
- Establishes a framework for coordinating the impact of an attack and its response with the business

**3. Review Who's Authorized to Make Changes to Your Policy.**

- Does the company currently employ all of them?
- Do they remain active members of the firewall management team?
- Have they received adequate training in the technology?
- Are they consistently undergoing ongoing technical training?
- Is there an established procedure for identifying and removing administrators who have departed from the organization or no longer possess firewall access rights? Is this process integrated with HR protocols?

**4. Review Your Firewall Change Procedures.**

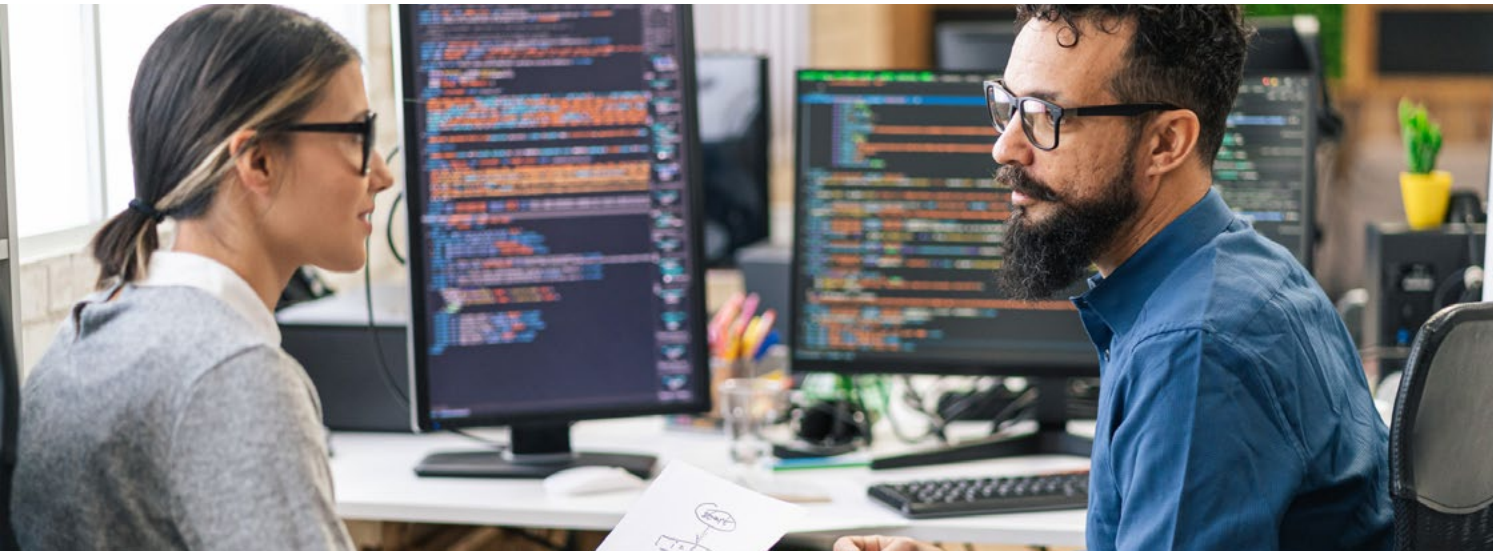
- Was the company's approval policy adhered to, and are the changes appropriately documented in the firewall rule base?
- How is the management of changes handled? What specific procedure is employed for receiving, tracking, approving, and verifying the completion of requests?
- Who provides authorization for firewall changes, and is there a formalized process for this with a documented audit trail?
- What mechanisms are in place for detecting unauthorized changes? Are all actual changes to the firewall thoroughly documented, providing a comprehensive audit trail? Can accountability for each change be demonstrated?

**5. Review Your Firewall System Design.**

- Is the organization's technology up-to-date? Is there a well-defined and documented procedure in place for technology upgrades?
- Have all the latest software versions been installed, and are patches applied regularly? While it doesn't need to be cutting-edge, a three-year gap is too long.
- Does the firewall rule base sufficiently safeguard the organization? If uncertain, reference the corporate security guidelines.
- Are the controls outlined in the written policy effectively enforced? Do you clearly understand the specific methods through which they are being enforced?

**6. Review Your Firewall Review Process.**

- Is the rule base subjected to a thorough review at least annually and preferably more frequently, ideally every quarter?
- Are redundant rules promptly identified and removed from the rule base?
- Do you regularly identify and eliminate unused regulations and objects from the rule base?
- Are rules that are overly permissive appropriately flagged for further investigation?
- Do you actively identify and assess risky traffic flows within the rule base?



## Step 2: Firewall Security Sets and Rule Overview

The second technical phase in a firewall audit typically involves thoroughly examining your rule base. This evaluation aims to determine whether your firewall operations are auditable and repeatable.

A firewall audit is a systematic process providing insight into your firewall's existing access and connections, vulnerability identification, and reporting on firewall changes, encompassing configuration, and real-time notifications.
Firewall rules and rulesets dictate handling both inbound and outbound network traffic, thereby regulating access to subnets and ensuring a secure network.

The four essential firewall rules that you should prioritize are:

1. **Deny All:** This rule defaults to denying all traffic unless explicitly permitted, thwarting unauthorized access and potential denial-of-service attacks.
2. **Least Privilege:** This rule permits only necessary network connections based on specific IP addresses, denying all other connections to ensure secure access to network devices.
3. **Explicit Allow:** This rule grants access to specific network traffic based on criteria such as source and destination addresses, type of service, TCP/UDP protocol, and authentication.
4. **Stateful Inspection:** This rule actively monitors the state of network connections, using this information to discern which network packets should be allowed through the firewall.

Implementing these rules, in conjunction with monitoring firewall logs, contributes to maintaining data security, controlling bandwidth, and bolstering the overall security posture of your network.

## Firewall Security Sets and Rule Overview Checklist

A firewall security set and rule checklist systematically assess and enhances the security posture of your organization's infrastructure, empowering your organization with the insights and guidelines necessary to fortify your defenses.

Here are the best practices for ensuring you meet firewall security sets and rules:

- **Perform Regular Firewall Audits**
  Conducting routine firewall audits is crucial to pinpoint misconfigurations, track policy changes, and ensure optimal functionality of the firewall device. Security audits are vital for administrators overseeing host-based or web server firewalls on Windows and Microsoft operating systems.

- **Establish a Robust Firewall Policy**
  A comprehensive firewall security policy is essential for effective management, covering router configuration, remote access, and gateway security. This is especially critical for achieving PCI DSS 4.0 compliance.

- **Deploying Advanced Firewall Solutions**
  Leveraging advanced solutions such as SecureTrack+ provides unparalleled visibility and in-depth analysis of firewall configurations. This enhances overall security management and fortifies defenses against threats like denial-of-service attacks.

- **Perform Regular Audits**
  Identity misconfigurations and policy changes, and check that your firewall is up-to-speed. Especially important for firewall administrators managing host-based or web server firewalls on Windows and Microsoft operating systems.

## Meet Compliance and Reduce Audit Fines with Tufin

Tufin minimizes the risk of failed audits by incorporating built-in, pre-flight compliance checks during network changes. The platform empowers you to produce customized firewall audit reports on demand, providing a centralized console for monitoring, maintaining, and demonstrating continuous compliance with industry regulations and internal policies across various components, including firewalls, routers, SDN, and hybrid cloud environments.

Tufin enables you to rapidly generate customizable audit reports to avoid audit fines, ensure continuous compliance by ensuring firewall audit readiness, and reduce audit preparation time from weeks to hours. In addition, Tufin stands out by offering support for thousands of firewalls, internal network devices, and cloud resources, consolidating audit readiness without the need for multiple tools.

### About Tufin

Tufin provides a single platform for network and cloud security teams to simplify the management of security policies across today's complex, multi-vendor hybrid networks. The platform gives some of the largest companies in the world the end-to-end visibility and automation tools necessary to swiftly provide new access, enable fast and secure application deployment, and ensure continuous compliance and audit readiness. Tufin's proven solutions help more than 2,000 customers across industries including healthcare, financial services, utilities, telecommunications and retail to quickly identify and mitigate network risks. For more information, please visit www.tufin.com.