Network Audit Checklist

Proactive Compliance and Security

Planning - Performing - Postprocessing. Network audits don't have to be a painful necessity that happen once a year. They are the result of an iterative process to ensure security, compliance and long-term growth. If you are planning a network audit, or simply frustrated with the amount of manual resources required for the activity, we have put together a checklist for you that will lay out some of the key steps and also make it clear how useful automated processes can be.

- **Network Inventory: Up-to-date and hands-free**
  In order to be able to make any declarations about the state of your network, it is essential to first get an overview of all elements in your network, from used software and hardware to the topological hierarchies of these elements.
- **Vulnerability Detection: Stay safe across vendors and technologies**
  You should always keep in mind that every vulnerability in your network is a potential point of attack! Therefore, it is essential to regularly check your network for vulnerabilities.
- **Lifecycle Management: Plan ahead for End of Life device series in your network**
  Device series that reach the end of their service or life (EoS/EoL) offer another potential point of attack. It is your responsibility to proactively identify and replace these devices.
- **Configuration Governance: Keep access privileged with clear roles**
  Reviewing the security of your network includes ensuring that access from external organizations meets the same minimum-security guidelines as those that you have for your internal infrastructure. Verifying the security of your data transmission and encryption therefore plays a major role.
- **Policy Compliance: Automated adherence to compliance requirements**
  As an organization, you have a number of policies and guidelines to comply with such as PCI-DSS, SOX, NSA, etc., but you also have internal requirements that you must meet. Verifying compliance with the requirements set in these policies should always be an integral part of your network audit.
- **Verify Configurations: Small errors can snowball into larger problems**
  Misconfigurations are one of the most common reasons for prolonged downtimes. To avoid this, you should regularly (and ideally with highly automated processes in place) review your configurations, create backups to track changes and compare different device configurations against one another.
- **SIEM Security Control: Compatibility to a wide range of control environments**
  The security of your network should be your top priority. A SIEM-compatible tool helps you filter huge amounts of security data to proactively detect and remediate incidents and allows you the flexibility to integrate a platform solution to your existing secure network environment.
- **Report Generation: Simplified, automated reporting to share insights**
  At the end of an audit, it is of utmost importance that you have detailed reports of your analysis. These help management and C-Level decision-makers, as well as external organizations that may need to follow up in the case of an incident.

Now you know what steps you need to go through to perform a comprehensive network audit. Of course, you can perform such an audit manually using various tools. However, this is time-consuming, resource-intensive and, above all, error-prone. Save resources and manage compliance with the consistent, reliable and highly-automated StableNet® Network and Service Management platform.
For more information about the audit process with StableNet®, read our use case or blog post.