Firewall Audit

autodata

Ensure your current firewall configuration and policies comply with all best practices and security standards

Industry Compliance

CIS - The Centre for Internet Security benchmark; reports can be run against Cisco ASA devices.

These reports have been externally certified by CIS and verified as auditing against their baseline.

www.cisecurity.org/cis-benchmarks

PCI - Payment Card Industry audits; perform the automatable system checks and support integrating this verified data with non-automatable policy checks.

Use Autodata's Firewall Audit Report to gather detailed results which offer advice, verify passes and explain failures, so you can quickly become compliant.

www.pcisecuritystandards.org/pci_security

STIG - U.S. Military compliance audit developed in conjunction with DoD IA user groups. Autodata uses leading tools favoured by many government and defence agencies to ensure reports are detailed, verifiable and include remediation in line with STIG baselines.

Reports can be generated offline for secure environments and scaled up to audit any number of devices.

SANS - A compliance audit against the SANS policy documents. The SANS institute is a trusted industry body which also trains information security professionals.

Their policy is a great compliance benchmark to audit against to assess your security level.

www.sans.org

The firewall is typically the centre of network security. **Autodata's Firewall Audit** provides an in-depth review of your configuration against best-practice standards - quickly and without the need to be connected to an online firewall.

Why should I audit my firewall?

Beyond compliance requirements, **firewall audits** are recommended for a very good reason: they increase your chances of catching any weaknesses in your network security posture and finding the places where your policies need to be adapted.

They also prove that you have been doing all your due diligence in reviewing your security and policy controls, should you ever need to respond to a breach or issue that brings your security standards into question.

Unfortunately it's all too common for firewall rules and security settings to be static over time. Firewalls are in need of continuous maintenance to supply the best security for your business, thus Autodata recommends regular firewall audits.

Service Overview

Autodata's technical consultants will conduct a review of your firewall configuration and rulesets: identifying, verifying and prioritising weaknesses against best practice.

Security Audit - Autodata will conduct a security audit against your firewall and look for weaknesses and vulnerabilities. We will look for the use of insecure technologies such as weak encryption protocols, easily cracked passwords (if stored in plaintext) and vulnerable network protocols.

Vulnerability Audit - Autodata will conduct a vulnerability audit on the firewall operating system, identifying known vulnerabilities and providing risk-based remediation advice.

CIS Benchmark Audit - Where available Autodata will check the configuration against a CIS benchmark for the OS, these are consensus-based configurations contributed to by security professionals around from around the world.

The audit reviews and measures your current configuration against industry standards, providing remediation steps to be taken for any highlighted risks.

256-260 Old Street, London, EC1V 9DD
t. +44 (0) 20 7749 7949 | e. salesteam@autodata.co.uk

Firewall Audit (cont'd)

Implementation Process

Our **Firewall Audit Report** can be generated using a copy of the firewall configuration and the public IP addresses of the firewall. This report will be exchanged via a secure encrypted file to ensure maximum security.

Autodata can also produce a more in-depth report by linking the audit to your network topology and providing a more detailed insight into your firewall configuration. Following report-generation, our technical team will take you through the report's content and any potential remediation steps to be taken.

Benefits

Autodata can produce reports quickly	Collate data quickly and get fast, actionable feedback.
We provide detailed technical and executive reporting for your organisation	Identify vulnerabilities on your network that you did not know existed and do something about it.
Remediation and mitigation advice	Understand why a vulnerability is an issue and plan how to fix it.
No network connection needed and offline activation	Non-intrusive process that doesn't require any set-up and can be used in locked-down environments. There is also an option to make use of online service discovery techniques for a more thorough audit.
Easy to understand and use	Autodata's reports are written in plain English making them easy to understand. Guidance is offered throughout the software to explain terminology and functions.

Supported Devices

256-260 Old Street, London, EC1V 9DD
t. +44 (0) 20 7749 7949 | e. salesteam@autodata.co.uk