

Rules Drift Over Time: Why Firewall Audits Matter

Keeping network access aligned with current business needs and member data protected.



A firewall is only as effective as the rules it enforces. Over time, business changes, temporary projects, previous vendor connections, and remote-access needs can leave behind rules that are no longer needed or overly permissive. Regular firewall rule audits help the credit union reduce unnecessary exposure, protect member information, and demonstrate that network access remains aligned with current business needs.

What an Effective Audit Should Test



Documented business purpose

Each rule should have a clear justification, owner, approval record, affected systems, and expected lifespan.



Unused rules

Remove or disable rules showing no legitimate traffic, after confirming they are not needed for periodic or contingency operations.



VPN architecture

Because SSL VPN services are frequently targeted, plan and execute migration to appropriately configured IPsec VPNs.



Protected management interfaces

Do not expose firewall administration interfaces directly to the Internet; restrict management access to trusted administrative paths.



Necessary traffic only

Restrict inbound and outbound traffic to the specific services, sources, destinations, ports, and protocols required to operate the credit union.



Secure VPN configuration

Use current encryption standards and eliminate weak or obsolete ciphers and protocols.



Remote-access identities

Require MFA, audit user accounts and privileges, limit access to business need, and promptly remove stale accounts.

These reviews reduce the chance that a forgotten rule, weak remote-access configuration, or compromised account becomes a path into the network. They also improve accountability by connecting technical access to a documented business decision and a responsible owner.



Next Steps

Direct IT, internal audit, or your managed service provider to review firewall rules and VPN access regularly—**no less than once per year**, and more often when systems, vendors, locations, or threats change. Require documented findings, rule owners, business purposes, approved exceptions, remediation actions, and completion dates. Management should receive a concise risk summary and verify that unnecessary access is removed and remaining issues are tracked to closure.