The 10 Firewall Weaknesses You Need to Find Before Attackers Do

Your network security controls drift every day, and you can't see it happening. As rules get added and altered, risk gets buried in the rulebase. Stale rules stay live, shadowed rules hide true exposure, and overly permissive any/any access sneaks into production.

Most teams have no reliable way to catch it. A handful of engineers govern 10 to 100 firewalls and hundreds of rule changes a week. Periodic manual reviews rarely confirm whether live controls still enforce the intended policy. Months pass between audits.

That gap is exactly what AI-powered attackers exploit. Modern environments change faster than any team can manually validate, and every misconfigured or drifted control becomes a hidden path to breach for would-be attackers.

HOW TO USE THIS CHECKLIST

CHECK AGAINST LIVE CONFIGURATION

The next few pages list 10 firewall controls that are commonly misconfigured. Check each one against your live configuration and security policy.

TICK ONLY WHAT IS ENFORCING

Tick a box only when you have confirmed that the control is properly configured and actively enforcing.

Every box left unchecked is a weakness to fix.

Score your firewall controls

Tick a box only when you've confirmed that the control is configured correctly and actively enforcing in production today - not merely present in policy.

- [ ] **01 URL FILTERING**

Unblocked suspicious categories let malware, phishing, and C2 sites reach users with no friction or logging.

- High-risk categories (C2, malware, phishing, ransomware) should be set to block
- Suspicious categories (new domains, dynamic DNS, parked) should be set to, at least, warn
- A filtering profile is attached to every internet-bound rule, with logging on

- [ ] **02 ANTIVIRUS**

Missing or alert-only antivirus lets known malware cross web, email, and file transfers untouched.

- An anti-malware profile is set to block (reset-both), not alert or default
- Every protocol is covered: HTTP/HTTP2, SMTP, IMAP, POP3, FTP, SMB
- The profile is applied to all rules carrying user and server traffic

- [ ] **03 DNS SIGNATURES**

Without DNS blocking, traffic to known-malicious domains resolves and connects unchecked.

- DNS signatures are enabled and set to block or sinkhole, not alert
- Coverage spans critical, high, and medium severity signatures
- Sinkholing is on so infected internal hosts show up in logs

- [ ] **04 OVERLY PERMISSIVE “ANY/ANY” RULE**

A firewall rule with source, destination, services, and applications all set to "Any" will potentially allow traffic that should be blocked. It shadows all policies beneath it in the ruleset, undermining the effectiveness of the overall security policy.

- No enabled rule has source, destination, application, and service set to Any
- Broad rules are scoped to specific hosts, users, and applications
- Rule order is reviewed so no permissive rule shadows those below it

- [ ] **05 INLINE ML — MALWARE DETECTION**

Signatures miss novel files; inline ML blocks never-before-seen malware in real time.

- Inline / real-time ML malware models are enabled and set to block
- All model types are on: executables, scripts, Linux ELF, Office docs
- Enabled across HTTP, SMTP, IMAP, POP3, FTP, and SMB

- [ ] **06 INLINE ML — PHISHING DETECTION**

Inline ML reads page content live to block phishing sites that URL categorization misses.

- Local / inline URL categorization is enabled on the profile
- The phishing-detection model is set to block, not alert
- The profile is applied to all user-facing internet rules

☐ 07 CLOUD SANDBOX — UNKNOWN FILE ANALYSIS

Unknown files must detonate in a sandbox; unforwarded, zero-day malware goes uncaught.

- Unknown files are forwarded to the cloud sandbox for analysis
- Forwarding covers all applications, file types, and both directions
- The analysis profile is attached to internet-facing rules

☐ 08 CLOUD SANDBOX — UNKNOWN URL ANALYSIS

Send unknown links to the sandbox so they are blocked as fresh verdicts land.

- Unknown URLs are forwarded to the cloud sandbox for analysis
- Coverage includes email-borne links, not just web browsing
- The analysis profile is attached to the relevant rules

☐ 09 DECRYPTION RULE DISABLED

A disabled decryption rule could allow traffic to pass through without inspection and visibility.

- Decryption rules are aligned to security policy and active
- Active decryption rules reduce the attack surface and bring clarity to the intent of the rulebase

☐ 10 FILE BLOCKING

No file-blocking policy means no brake on risky executables, scripts, and archives.

- High-risk types are blocked (archives, scripts, HTA, JAR, PIF, SCR, ISO, torrents)
- Blocking applies in both directions (upload and download)
- Scoped to the right apps (email + web), with action set to block

YOUR SCORE — BOXES CHECKED OUT OF 10

0–4 CHECKED

Significant exposure. Multiple attack paths are open in your environment right now.

5–8 CHECKED

Partial coverage. You'll stop some attacks, but real gaps remain to close.

9–10 CHECKED

Strong posture. Keep validating as policies, rules, and threats change.

Find and fix firewall misconfigurations.
Before attackers exploit them.

See how Reach provides continuous assurance across your network security controls.

Request a Demo