WELT 12: INFRASTRUKTUR-NEBEL · MISSION 12.2

Firewall-Regeln im Röntgenblick

Seit dem «kleinen Umbau» geht das Internet nicht – nur die Wartungsfirma jubelt. Sie röntgen ein Übungs-Regelwerk mit KI und finden elf Lücken, bevor es jemand anderes tut.

Zur Mission

DAUER 60 Min. KOSTEN Gratis WERKZEUGE OpenAI Codex, Claude (Web), ChatGPT, Google Gemini DATENAMPEL Grün – unbedenklich

Das Wichtigste

- nftables: input = an die Firewall, forward = durch die Firewall. policy drop = was nicht erlaubt ist, ist verboten.
- Erste passende Regel gewinnt. Spezifische Sperren vor allgemeine Erlaubnisse – sonst sind sie verdeckt.
- Ohne «ct state established,related accept» kommen bei policy drop keine Antworten zurück.
- Der KI immer Regelwerk UND Sollregeln geben; pro Befund eine Regelnummer verlangen.
- Pakete Regel für Regel durchspielen lassen und selbst nachprüfen – das entlarvt Floskeln.
- Suggestivfragen («R11 sperrt doch, oder?») verleiten die KI zum Zustimmen. Offen fragen.
- Änderungen nur als Vorschlag: Sicherung, Prüfung ohne Laden, zweite Person, Rückfall, Tests. Ausführen tut die verantwortliche Person.
- Echte Regelwerke sind vertraulich: nur mit Freigabe, mit ersetzten Adressen oder lokal auswerten.

Ihr Produkt

Ein ausgefüllter **Röntgen-Befundbogen** für ein Firewall-Regelwerk und ein **Verbesserungsvorschlag mit Rückfallplan**; als Kür (optional) ein selbst erzeugter **Fehlerfall für Lernende** (Regelwerk mit eingebauten Lücken plus Lösung).

Abnahme: Ihr Befundbogen enthält mindestens sechs Befunde mit Regelnummer und Sollregel, darunter die verdeckte Regel R11 und die Ursache der Störung, und Ihr Verbesserungsvorschlag enthält Sicherung, Test und Rückfallplan statt eines Befehls zum sofortigen Laden. Wer die Kür macht: Die eingebauten Fehler im Fehlerfall für Lernende sind gegen die Lösung geprüft.

So gehen Sie vor

1. Drei Minuten Röntgenblick – ohne KI
2. Auf den Röntgentisch
3. Paket-Detektiv: Wer lässt wen durch?
4. Befundbogen: einstufen und gegenprüfen
5. Vorschlag mit Rückfallplan statt Schnellschuss
6. Kür (optional, +20 Minuten): Fehlerfall für Lernende

Start-Prompt

Du bist eine erfahrene Netzwerk- und Sicherheitsfachperson. Prüfe das folgende nftables-Regelwerk einer fiktiven Schule gegen die Sollregeln.
Sollregeln und Netzplan: [INHALT VON uebungsnetz-plan.md]
Regelwerk: [INHALT VON uebungsnetz-regeln.nft]
Liefere eine Tabelle: Regelnummer | Befund | verletzte Sollregel | Stufe (kritisch, wichtig, Kosmetik) | Begründung in einem Satz.
Prüfe ausdrücklich: Reihenfolge und verdeckte Regeln, fehlende Regeln, zu breite Quellen oder Ziele, Kommentare, die nicht zum Inhalt passen, abgelaufene Befristungen, unbenutzte Definitionen.
Erkläre danach die drei Störungsmeldungen: Warum geht das Internet nicht, und warum funktioniert bei der Wartungsfirma alles?
Schlage noch keine Änderungen vor. Schweizer Rechtschreibung (immer «ss», kein Eszett).

Qualitätscheck

- Jeder Befund nennt eine Regelnummer und eine Sollregel; nichts ist bloss «allgemeiner Tipp».
- Die verdeckte Regel R11 und die fehlende Rückweg-Regel (Ursache der Störung) sind gefunden und erklärt.
- Sie haben mindestens ein Paket selbst Regel für Regel nachverfolgt und das Ergebnis der KI bestätigt oder widerlegt.
- Der Verbesserungsvorschlag enthält Sicherung, Prüfung ohne Laden, zweite Person, Rückfall und Tests – und keinen Aufruf, die Regeln selbst zu laden.
- Echte Regelwerke Ihrer Schule sind in keine Cloud-KI gelangt (oder nur mit Freigabe und ersetzten Adressen).
- Kür: Im Fehlerfall für Lernende stecken genau die bestellten Fehler – geprüft gegen die Lösung, ohne zusätzliche, unbeabsichtigte Fehler.

Hängen Sie fest? Frag die KI

Ich bin Lehrperson an einer Schweizer Berufsfachschule und lerne, Firewall-Regeln zu lesen. Erkläre mir einfach, was bei nftables «table», «chain», «hook input» und «hook forward», «policy drop» und «policy accept» bedeuten und warum die Reihenfolge der Regeln wichtig ist. Nimm als Beispiel eine Schule mit einem Netz für Lernende und einem für die Verwaltung. Nenne mir Suchbegriffe für die offizielle nftables-Dokumentation (keine Links erfinden).

Klappt nicht? Das Regelwerk ist fiktiv und kurz: Sie können es in jede Gratis-KI im Browser einfügen (ChatGPT, Claude, Gemini, Copilot). Mit Codex (Gratis-ChatGPT-Konto genügt) liest der Agent die Dateien direkt im Übungsordner. Für echte Regelwerke Ihrer Schule: nur mit Freigabe des Informatikdienstes und ohne öffentliche Adressen und Namen – oder lokal mit LM Studio.

Stand 19.11.2026 · CC BY 4.0 Alpasana GmbH · Werkzeuge ändern sich – prüfen Sie selbst.