MikroTik für Anfänger - Teil 3

Firewall & Sicherheit

MikroTik für Anfänger - Teil 3

Firewall & Sicherheit

Inhalt

Willkommen zum Finale! Dein Netzwerk läuft (Teil 1 & 2). Aber ist es auch sicher?

Ein MikroTik-Router ist ein mächtiges Werkzeug. Aber im Gegensatz zu Consumer-Routern (die oft alles automatisch blockieren), macht MikroTik nur das, was du ihm sagst. Wenn du nichts sagst, ist er oft “offen”.

In diesem Teil bauen wir deine digitale Festung.

---

1. Firewall-Grundlagen: Input vs. Forward

Die Firewall von MikroTik unterscheidet zwei Haupt-Richtungen (“Chains”), die du verstehen musst:

- **Input Chain:** Alles, was **AN den Router selbst** geschickt wird.

    - Beispiel: Du willst dich per WinBox einloggen. Ein Hacker versucht, dein Router-Passwort zu erraten.
    - Ziel: Wir wollen nur Zugriff aus dem LAN erlauben, niemals aus dem Internet (WAN)!
- **Forward Chain:** Alles, was **DURCH den Router hindurch** geht.
    - Beispiel: Dein PC surft im Internet. Ein Hacker versucht, auf deine Überwachungskamera zuzugreifen.
    - Ziel: Wir wollen, dass LAN ins Internet darf, aber das Internet NICHT ins LAN.

---

2. Die “Eiserne Regel” (Drop all from WAN)

Das ist die wichtigste Regel überhaupt. Sie besagt: “Alles, was von draußen (Internet) kommt und nicht angefordert wurde, wird weggeworfen (Drop).”

Einrichtung in WinBox:

1. Gehe zu `IP` -> `Firewall` -> Reiter `Filter Rules`.
2. Klicke auf `+`.
3. **General** Reiter:
    - Chain: `input`
    - In. Interface: `ether1` (oder `pppoe-out1`, dein Internet-Interface!)
    - Connection State: Haken bei `new`.
4. **Action** Reiter:
    - Action: `drop`
5. `OK` klicken.

Wiederhole das Ganze für die `forward` Chain! (Chain: `forward`, In. Interface: `ether1`, Action: `drop`).

Achtung: Bevor du diese “Drop”-Regeln aktivierst, musst du sicherstellen, dass du eine Regel hast, die “Established & Related” Verbindungen erlaubt. Sonst sperrst du auch deine eigenen Antworten aus dem Internet aus!

Die Standard-Konfiguration ("DefConf") von MikroTik hat diese Regeln meist schon. Prüfe es nach! Wenn du Regeln siehst wie "defconf: drop all not coming from LAN", bist du sicher.

---

3. Port-Weiterleitung (NAT)

Manchmal WILLST du aber von außen zugreifen. Zum Beispiel auf deinen **Home Assistant**, wenn du unterwegs bist. Dafür bohren wir ein kontrolliertes Loch in die Firewall. Das nennt man **Destination NAT** (Dst-NAT).

Beispiel: Home Assistant (Port 8123) freigeben

1. Gehe zu `IP` -> `Firewall` -> Reiter `NAT`.
2. Klicke auf `+`.
3. **General** Reiter:
   - Chain: `dstnat` (Destination NAT).
   - Protocol: `6 (tcp)`.
   - Dst. Port: `8123` (Der Port, den du von außen ansprichst).
   - In. Interface: `ether1` (Dein Internet-Eingang).
4. **Action** Reiter:
   - Action: `dst-nat`.
   - To Addresses: `192.168.88.XX` (Die interne IP deines Home Assistant).
   - To Ports: `8123`.
5. `OK` klicken.

Sicherheits-Warnung: Jede Port-Weiterleitung ist ein Risiko! Wenn dein Home Assistant ein schwaches Passwort hat, ist der Hacker drin.

- Besser: Nutze VPN (WireGuard), um dich sicher nach Hause zu verbinden, statt Ports zu öffnen. (Thema für einen Profi-Kurs!).

Abschluss

Herzlichen Glückwunsch! Du hast es geschafft. Du hast von Null angefangen und besitzt jetzt ein professionell verkabeltes, konfiguriertes und abgesichertes MikroTik-Netzwerk.

Du gehörst jetzt zu den “Prosumern”. Dein Netzwerk ist stabiler, schneller und sicherer als das von 99% deiner Nachbarn.

Viel Spaß mit deinem neuen High-End-Heimnetzwerk!