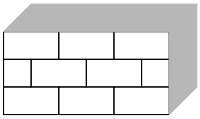
**informationstechnikj2-bpe10.1g-firewallung**

## Komplikation

Um ein hohes Maß an *Sicherheit* in Netzwerken zu realisieren, benutzen wir Netzwerkdienste und *Firewalls* um gezielt Ports zu schließen beziehungsweise zu öffnen und die transportierten Datenpakete zu überwachen:



Mögliche Befehle für die Transportüberwachung eines Firewalls sind:

- ALLOW:
- DROP:
- REJECT:

| Parameter | Beschreibung |
|---|---|
| Interface | WAN, LAN, VLANxx (z.B. VLAN01, VLAN10) |
| Version | Protokollversion (IPv4 oder IPv6 oder beides IPv4+6) |
| Protokoll | Protokolltyp (z.B. UDP, TCP) |
| Quelle | IP-Adresse, Adressbereich, lokale Rechnernamen, Domainnamen, MAC-Adressen. Invertierung mit vorangestelltem Ausrufezeichen (!) möglich. |
| Quellport(s) | Wert(e) des Quellports im Paket (einzelne Ports, z.B. 80, mehrere Ports durch Komma getrennt, z.B. 80, 8080 oder Portbereiche, z.B. 9000-65535) |
| Ziel | wie Quelle, nur für die Ziele im Paket |
| Zielport(s) | wie Quellport, nur für den Zielport |

Eine Regel baut sich dabei wie folgt auf:

Befehl Interface Version Protokoll Quelle Quellport Ziel Zielport

Zur Optimierung der Sicherheit in Netzwerken verwendet man auch:

- *DMZ*:
- *Portfilter*:

## Retardation

### Aufgabe 1

Erläutere jeweils die Funktionsweise der Firewall-Regel.

1. ALLOW VLAN10 IPv4 ANY ANY ANY ANY ANY
2. DROP LAN IPv4+6 dbserver TCP ANY ANY ANY
3. DROP LAN IPv4+6 172.16.0.0/24 ANY 80, 8080 ANY ANY
4. ALLOW WLAN IPv4+6 ANY matheliebsch.de ANY ANY ANY
5. REJECT WLAN IPv4+6 TCP !matheliebsch.de ANY ANY ANY

### Aufgabe 2

Beschreibe jeweils.

1. Funktionsweise eines Portfilters und Relevanz für die Netzwerksicherheit.
2. Funktionsweise einer DMZ und Relevanz für die Netzwerksicherheit.