ufw

context

dit document beschrijft de werking van ufw, uncomplicated firewall.
standaard staat de firewall uit. Als je die ativeert, zijn dit de standaard waarden:

1. inkomend: deny
2. uitgaand: allow
3. forward: deny

status

- algemene status:

```
sudo ufw status verbose
```

- overzicht actieve regels:

```
sudo ufw status numbered
```

- begin met een reset van de config:

```
ufw reset
```

verkeer toestaan

```
sudo ufw allow in proto <protocol> from <source ip> to any port <poort>
comment "beschrijving"
```

voorbeeld:

```
sudo ufw allow in proto tcp from 10.0.1.20/32 to any port 5601 comment
"Access to Kibana"
```

verkeer blokkeren

```
sudo ufw deny from <ip adres> to any
```

voorbeeld:

```
sudo ufw deny from 10.11.12.13 to any
```

applicatie profielen

- staan onder /etc/ufw/applications.d/
- bevatten standaard instellingen voor programma'd die je installeert (vg nginx, openssh, ...)
- overzicht:

  ```
  ufw app list
  ```

- regels aanmaken:

  ```
  ufw allow "Nginx HTTPS"
  ```

service beheer

in-/uitschakelen:

```
sudo ufw enable|disable
```

servicebeheer

```
sudo systemctl start|stop|status ufw
```

regels verwijderen

1. zoek het regelnummer op:

   ```
   sudo ufw status numbered
   ```

2. verwijder de regel:

   ```
   sudo ufw status delete <regelnummer>
   ```

configuratie

- /etc/ufw

logging

- /var/log/ufw.log.
  Vereist wel dat je logging actief hebt:

```
sudo ufw logging on && sudo ufw reload
```

problemen, problemen

1. kijk logging na: <>

```
sudo tail -f /var/log/ufw.log
```

meer info

artikel Digital Ocean

Linux, firewall