Linux mit ufw (Uncomplicated FireWall) absichern

Installation

UFW installieren:

```
apt install ufw
```

IPv6 bei Bedarf deaktivieren

Editieren der Datei /etc/default/ufw:

```
nano /etc/default/ufw
```

Um IPv6 zu deaktivieren, ändern der Zeile IPV6=yes auf IPV6=no:

```
# /etc/default/ufw
#

# Set to yes to apply rules to support IPv6 (no means only IPv6 on loopback
# accepted). You will need to 'disable' and then 'enable' the firewall for
# the changes to take affect.
IPV6=no
```

Aufrufen der Hilfe

```
ufw help
```

```
Usage: ufw COMMAND

Commands:
 enable                          enables the firewall
```

```
 disable                           disables the firewall
 default ARG                       set default policy
 logging LEVEL                     set logging to LEVEL
 allow ARGS                        add allow rule
 deny ARGS                         add deny rule
 reject ARGS                       add reject rule
 limit ARGS                        add limit rule
 delete RULE|NUM                   delete RULE
 insert NUM RULE                   insert RULE at NUM
 route RULE                        add route RULE
 route delete RULE|NUM             delete route RULE
 route insert NUM RULE             insert route RULE at NUM
 reload                            reload firewall
 reset                             reset firewall
 status                            show firewall status
 status numbered                   show firewall status as numbered list of RULES
 status verbose                    show verbose firewall status
 show ARG                          show firewall report
 version                           display version information

Application profile commands:
 app list                          list application profiles
 app info PROFILE                  show information on PROFILE
 app update PROFILE                update PROFILE
 app default ARG                   set default application policy
```

Vorgefertigte Profile

Die ufw hat vorgefertigte Profile für verschiedene Dienste:

```
ufw app list
```

```
Available applications:
  AIM
  Bonjour
  CIFS
  DNS
  Deluge
  IMAP
  IMAPS
```

```
  IPP
  KTorrent
  Kerberos Admin
  Kerberos Full
  Kerberos KDC
  Kerberos Password
  LDAP
  LDAPS
  LPD
  MSN
  MSN SSL
  Mail submission
  NFS
  OpenSSH
  POP3
  POP3S
  PeopleNearby
  SMTP
  SSH
  Socks
  Telnet
  Transmission
  Transparent Proxy
  VNC
  WWW
  WWW Cache
  WWW Full
  WWW Secure
  XMPP
  Yahoo
  qBittorrent
  svnserve
```

Die Dienste verwenden die Standardports, so z.B. Port 22 für SSH, Port 80 für WWW oder Port 443 für WWW Secure.

Weitere Informationen bezüglich der Ports finden sich in den Konfigurationsdateien im Verzeichnis /etc/ufw/applications.d:

```
ls -al /etc/ufw/applications.d
```

```
insgesamt 52
drwxr-xr-x 2 root root 4096 Jun  7 13:58 .
drwxr-xr-x 3 root root 4096 Feb  7  2018 ..
-rw-r--r-- 1 root root  145 Nov 18  2017 openssh-server
-rw-r--r-- 1 root root  353 Feb 18  2016 ufw-bittorent
-rw-r--r-- 1 root root  627 Feb 18  2016 ufw-chat
-rw-r--r-- 1 root root  513 Feb 18  2016 ufw-directoryserver
-rw-r--r-- 1 root root   89 Feb 18  2016 ufw-dnsserver
-rw-r--r-- 1 root root  358 Feb 18  2016 ufw-fileserver
-rw-r--r-- 1 root root  212 Feb 18  2016 ufw-loginserver
-rw-r--r-- 1 root root  524 Feb 18  2016 ufw-mailserver
-rw-r--r-- 1 root root  131 Feb 18  2016 ufw-printserver
-rw-r--r-- 1 root root  155 Feb 18  2016 ufw-proxyserver
-rw-r--r-- 1 root root  320 Feb 18  2016 ufw-webserver
```

```
cat ufw-webserver
```

```
[WWW]
title=Web Server
description=Web server
ports=80/tcp

[WWW Secure]
title=Web Server (HTTPS)
description=Web Server (HTTPS)
ports=443/tcp

[WWW Full]
title=Web Server (HTTP,HTTPS)
description=Web Server (HTTP,HTTPS)
ports=80,443/tcp

[WWW Cache]
title=Web Server (8080)
description=Web Server (8080)
ports=8080/tcp
```

Die Konfigurationsdateien in diesem Verzeichnis können durch eigene Einträge ergänzt oder es können auch neue Konfigurationsdateien erstellt werden.

Regeln hinzufügen

In diesem Beispiel wird der SSH-Zugang für das lokale Netzwerk (192.168.1.0/24) und ein Webzugriff für jede IP eingerichtet, IPv6 wurde deaktiviert:

```
ufw allow from 192.168.1.0/24 to any app SSH
```

```
ufw allow 'WWW Full'
```

Die Firewall starten:

```
ufw enable
```

Die Durchführung mit ‚y' bestätigen:

```
Command may disrupt existing ssh connections. Proceed with operation (y|n)? y
Firewall is active and enabled on system startup
```

Status abfragen

```
ufw status
```

```
Status: active

To                         Action      From
--                         ------      ----
SSH                        ALLOW       192.168.1.0/24
WWW Full                   ALLOW       Anywhere
```

Einen detailierten Status mit Angabe der Ports ausgeben:

```
ufw status verbose
```

```
Status: active
Logging: on (low)
Default: deny (incoming), allow (outgoing), disabled (routed)
New profiles: skip

To                         Action      From
--                         ------      ----
22/tcp (SSH)               ALLOW IN    192.168.1.0/24
```

```
80,443/tcp (WWW Full)      ALLOW IN    Anywhere
```

Löschen von Regeln

Ausgabe des Status mit Nummern:

```
ufw status numbered
```

```
Status: active

     To                         Action      From
     --                         ------      ----
[ 1] SSH                        ALLOW IN    192.168.1.0/24
[ 2] WWW Full                   ALLOW IN    Anywhere
```

Löschen der Regel über die Nummer:

```
ufw delete 2
```

Beispiele

Eingehende Pakete auf Port 12345 zulassen:

```
ufw allow from 192.168.1.0/24 to any port 12345
```

Eingehende UDP Pakete auf Port 54321 zulassen:

```
ufw allow from 192.168.1.0/24 proto udp to any port 54321
```

Eine neue Regel an erster Postition einfügen:

```
ufw prepend allow from ...
```

Eine neue Regel an der Position 2 einfügen:

```
ufw insert 2 allow from ...
```

> Standardmäßig werden ausgehende Pakete immer akzeptiert. Um dies zu ändern muss die Einstellung in der **/etc/default/ufw** auf **DEFAULT_OUTPUT_POLICY="DROP"** geändert werden.

Ausgehende Pakete zu 192.168.1.1 blocken:

```
ufw deny out from any to 192.168.1.1
```

Ausgehende DNS Anfragen (Port 123/UDP) an 192.168.1.1 zulassen:

```
ufw allow out to 192.168.1.1 port 123 proto udp
```

Revision #14
Created 2026-01-11 19:17:49 UTC by Admin
Updated 2026-04-07 20:48:58 UTC by Admin