Inhaltsverzeichnis

UFW Firewall

Installation und Status

iptables2 ist eine Firewall Einrichtungen bei Ubuntu oder Debian. Eine vereinfachte Version ist ufw .

```
sudo apt-get update // Software update starten.
sudo -s // root Rechte erlangen, Sie müssendas root Passort eingeben.
apt-get install ufw // Startet die Installation von ufw
```

Mit folgendem Befehlt lässt sich die Einstellungen der Firewall anzeigen lassen.

```
ufw status // Beispielausgabe:

root@HPGen10-1:~# ufw status
Status: active

To                         Action      From
--                         ------      ----
OpenSSH                    ALLOW       Anywhere
22/tcp                     ALLOW       Anywhere
OpenSSH (v6)               ALLOW       Anywhere (v6)
22/tcp (v6)                ALLOW       Anywhere (v6)

root@HPGen10-1:~#
```

Wo wird was gespeichert ?

Die Einstellungen werden in folgenden drei Dateien gespeichern:

1. /etc/ufw/**before.rules**
2. /var/lib/ufw/**user.rules** (oder /lib/ufw/user.rules - in welche auch die in der Kommandozeile definierten Regeln persistiert werden)
3. /etc/ufw/**after.rules**

Diese Dateien lassen sich mit jedem Texteditor wie zum Beispiel nano verwalten. Hier eine Beispielausgabe der Datei: **/etc/ufw/before.rules**

```
root@HPGen10-1:~# root@HPGen10-1:~# cat /etc/ufw/before.rules
#
# rules.before
#
# Rules that should be run before the ufw command line added rules. Custom
# rules should be added to one of these chains:
#   ufw-before-input
#   ufw-before-output
```

```
#   ufw-before-forward
#

# Don't delete these required lines, otherwise there will be errors
*filter
:ufw-before-input - [0:0]
:ufw-before-output - [0:0]
:ufw-before-forward - [0:0]
:ufw-not-local - [0:0]
# End required lines


# allow all on loopback
-A ufw-before-input -i lo -j ACCEPT
-A ufw-before-output -o lo -j ACCEPT

# quickly process packets for which we already have a connection
-A ufw-before-input -m conntrack --ctstate RELATED,ESTABLISHED -j ACCEPT
-A ufw-before-output -m conntrack --ctstate RELATED,ESTABLISHED -j ACCEPT
-A ufw-before-forward -m conntrack --ctstate RELATED,ESTABLISHED -j ACCEPT

# drop INVALID packets (logs these in loglevel medium and higher)
-A ufw-before-input -m conntrack --ctstate INVALID -j ufw-logging-deny
-A ufw-before-input -m conntrack --ctstate INVALID -j DROP

# ok icmp codes for INPUT
-A ufw-before-input -p icmp --icmp-type destination-unreachable -j ACCEPT
-A ufw-before-input -p icmp --icmp-type time-exceeded -j ACCEPT
-A ufw-before-input -p icmp --icmp-type parameter-problem -j ACCEPT
-A ufw-before-input -p icmp --icmp-type echo-request -j ACCEPT

# ok icmp code for FORWARD
-A ufw-before-forward -p icmp --icmp-type destination-unreachable -j ACCEPT
-A ufw-before-forward -p icmp --icmp-type time-exceeded -j ACCEPT
-A ufw-before-forward -p icmp --icmp-type parameter-problem -j ACCEPT
-A ufw-before-forward -p icmp --icmp-type echo-request -j ACCEPT

# allow dhcp client to work
-A ufw-before-input -p udp --sport 67 --dport 68 -j ACCEPT

#
# ufw-not-local
#
-A ufw-before-input -j ufw-not-local

# if LOCAL, RETURN
-A ufw-not-local -m addrtype --dst-type LOCAL -j RETURN

# if MULTICAST, RETURN
-A ufw-not-local -m addrtype --dst-type MULTICAST -j RETURN
```

```
# if BROADCAST, RETURN
-A ufw-not-local -m addrtype --dst-type BROADCAST -j RETURN

# all other non-local packets are dropped
-A ufw-not-local -m limit --limit 3/min --limit-burst 10 -j ufw-logging-deny
-A ufw-not-local -j DROP

# allow MULTICAST mDNS for service discovery (be sure the MULTICAST line
above
# is uncommented)
-A ufw-before-input -p udp -d 224.0.0.251 --dport 5353 -j ACCEPT

# allow MULTICAST UPnP for service discovery (be sure the MULTICAST line
above
# is uncommented)
-A ufw-before-input -p udp -d 239.255.255.250 --dport 1900 -j ACCEPT

# don't delete the 'COMMIT' line or these rules won't be processed
COMMIT
root@HPGen10-1:~#
```

Hier eine Beispielausgabe der Datei: **/etc/ufw/user.rules**

```
root@HPGen10-1:~# root@HPGen10-1:~# cat /etc/ufw/user.rules
*filter
:ufw-user-input - [0:0]
:ufw-user-output - [0:0]
:ufw-user-forward - [0:0]
:ufw-before-logging-input - [0:0]
:ufw-before-logging-output - [0:0]
:ufw-before-logging-forward - [0:0]
:ufw-user-logging-input - [0:0]
:ufw-user-logging-output - [0:0]
:ufw-user-logging-forward - [0:0]
:ufw-after-logging-input - [0:0]
:ufw-after-logging-output - [0:0]
:ufw-after-logging-forward - [0:0]
:ufw-logging-deny - [0:0]
:ufw-logging-allow - [0:0]
:ufw-user-limit - [0:0]
:ufw-user-limit-accept - [0:0]
### RULES ###

### tuple ### allow tcp 22 0.0.0.0/0 any 0.0.0.0/0 OpenSSH - in
-A ufw-user-input -p tcp --dport 22 -j ACCEPT -m comment --comment
'dapp_OpenSSH'

### tuple ### allow tcp 22 0.0.0.0/0 any 0.0.0.0/0 in
-A ufw-user-input -p tcp --dport 22 -j ACCEPT
```

```
### END RULES ###

### LOGGING ###
-A ufw-after-logging-input -j LOG --log-prefix "[UFW BLOCK] " -m limit --
limit 3/min --limit-burst 10
-A ufw-after-logging-forward -j LOG --log-prefix "[UFW BLOCK] " -m limit --
limit 3/min --limit-burst 10
-I ufw-logging-deny -m conntrack --ctstate INVALID -j RETURN -m limit --
limit 3/min --limit-burst 10
-A ufw-logging-deny -j LOG --log-prefix "[UFW BLOCK] " -m limit --limit
3/min --limit-burst 10
-A ufw-logging-allow -j LOG --log-prefix "[UFW ALLOW] " -m limit --limit
3/min --limit-burst 10
### END LOGGING ###

### RATE LIMITING ###
-A ufw-user-limit -m limit --limit 3/minute -j LOG --log-prefix "[UFW LIMIT
BLOCK] "
-A ufw-user-limit -j REJECT
-A ufw-user-limit-accept -j ACCEPT
### END RATE LIMITING ###
COMMIT
root@HPGen10-1:~#
```

Hier eine Beispielausgabe der Datei: **/etc/ufw/after.rules**

```
root@HPGen10-1:~# root@HPGen10-1:~# cat /etc/ufw/after.rules
#
# rules.input-after
#
# Rules that should be run after the ufw command line added rules. Custom
# rules should be added to one of these chains:
#   ufw-after-input
#   ufw-after-output
#   ufw-after-forward
#

# Don't delete these required lines, otherwise there will be errors
*filter
:ufw-after-input - [0:0]
:ufw-after-output - [0:0]
:ufw-after-forward - [0:0]
# End required lines

# don't log noisy services by default
-A ufw-after-input -p udp --dport 137 -j ufw-skip-to-policy-input
-A ufw-after-input -p udp --dport 138 -j ufw-skip-to-policy-input
-A ufw-after-input -p tcp --dport 139 -j ufw-skip-to-policy-input
-A ufw-after-input -p tcp --dport 445 -j ufw-skip-to-policy-input
```

```
-A ufw-after-input -p udp --dport 67 -j ufw-skip-to-policy-input
-A ufw-after-input -p udp --dport 68 -j ufw-skip-to-policy-input

# don't log noisy broadcast
-A ufw-after-input -m addrtype --dst-type BROADCAST -j ufw-skip-to-policy-
input

# don't delete the 'COMMIT' line or these rules won't be processed
COMMIT
root@HPGen10-1:~#
```

Einige Beispielanwendungen