

# SSH vor Brute-Force-Angriffen härten

Um den SSH-Zugang im Internet zu schützen gibt es verschiedene Möglichkeiten:

- DenyHost (Python-script)
- Fail2ban (python-script)
- recent (kernelmodul von iptables)

DenyHost und Fail2ban müssen einfach nur mittels „apt-get install“ installiert werden, eine Änderung der Standardkonfiguration ist im Normalfall nicht notwendig.

recent ist bereits bei der Standardinstallation enthalten, allerdings müssen einige IP-Tables regeln zur laufzeit erstellt werden:

## secureSSHWithIptables

```
#!/bin/bash

# SSH erlauben - aber vor bruteforce schützen
iptables -N SSH-BruteForce
iptables -N SSH-Whitelist

iptables -A SSH-BruteForce -p tcp --dport 22 -m state --state NEW -m
recent --set --name ssh
iptables -A SSH-BruteForce -p tcp --dport 22 -m state --state NEW -j
SSH-Whitelist

iptables -A SSH-BruteForce -p tcp --dport 22 -m state --state NEW -m
recent --update --seconds 600 --hitcount 4 --rttl --name ssh -j DROP

iptables -I INPUT -j SSH-BruteForce

#whitelist
iptables -A SSH-Whitelist -s 10.42.0.12 -m recent --remove --name ssh -
j ACCEPT

exit 0
```

In der Datei „/proc/net/xt\_recent/ssh“ werden die BruteForce-Attacken mit IP's geloggt.

From:  
<http://dbcc.fh-schmalkalden.de/wiki-dbcc/> - **DBCC-Wiki**

Permanent link:  
<http://dbcc.fh-schmalkalden.de/wiki-dbcc/manton:linux:securessh?rev=1504689151>

Last update: **2017/09/06 11:12**



