

## IP-Ranges blockieren mit Suse Firewall

Zum Blockieren von dubiosen IP-Ranges empfiehlt sich der Einsatz der Firewall.

Andere Mechanismen wie z.B. "hosts.allow/hosts.deny" funktionieren nur teilweise – nicht z.B. bei Apache Webservern und auch nicht bei Suse Linux SSH.

Vorgehensweise:

1. Aktivierung der Suse Firewall 2 in YAST
2. "custom scripts" in der Datei /etc/sysconfig/scripts/SuSEfirewall2-custom anpassen unter dem Schlüssel `fw_custom_before_denyall()`— hier der Auszug aus der Datei /etc/sysconfig/scripts/SuSEfirewall2-custom—

```
....  
fw_custom_before_denyall() { # could also be named "after_forwardmasq()"  
# these are the rules to be loaded after IP forwarding and masquerading  
# but before the logging and deny all section is set by SuSEfirewall2.  
# You can use this hook to prevent the logging of annoying packets.
```

```
# Drop following source ranges  
iptables -A INPUT -j DROP -s 61.146.0.0/16  
iptables -A INPUT -j DROP -s 61.174.0.0/16  
iptables -A INPUT -j DROP -s 113.171.0.0/16  
iptables -A INPUT -j DROP -s 116.10.0.0/16  
iptables -A INPUT -j DROP -s 125.76.0.0/16  
iptables -A INPUT -j DROP -s 181.110.0.0/16
```

3. In der Datei /etc/sysconfig/SuSEfirewall2 den Pfad zur custom rule wie folgt aktivieren:  
# This is really an expert option. NO HELP WILL BE GIVEN FOR THIS!  
# READ THE EXAMPLE CUSTOMARY FILE AT /etc/sysconfig/scripts/SuSEfirewall2-custom  
#  
`FW_CUSTOMRULES="/etc/sysconfig/scripts/SuSEfirewall2-custom"`  
#FW\_CUSTOMRULES=""
4. Firewall stoppen und wieder starten um neue Rule zu aktivieren!  
SuSEfirewall2 stop  
SuSEfirewall2 start

Fertig!

Zusätzlich könnte man noch die SSH-Logins und Login-Versuche beschränken auf 3 Stück pro Minute:

- `iptables -I INPUT -p tcp -dport 22 -i eth0 -m state --state NEW -m recent --set`
- `iptables -I INPUT -p tcp -dport 22 -i eth0 -m state --state NEW -m recent --update --seconds 60 --hitcount 3 -j DROP`

Quelle: <http://dahlmann.biz/wordpress/?p=569>

Eindeutige ID: #1080

Verfasser: n/a

Letzte Änderung: 2018-05-09 10:03