iptables

Revert to iptables legacy on Debian

- Rucne zvolit variantu `update-alternatives --config iptables`
- Revertnout na legacy rezim `update-alternatives --set iptables /usr/sbin/iptables-legacy`
- Zrusit revert a pouzit Debian default `update-alternatives --auto iptables`

GeoIP modul

Nainstalujeme modul xt_geoip

- `apt-get install iptables-dev xtables-addons-common libtext-csv-xs-perl pkg-config`

V adresari **/usr/lib/xtables-addons** spustime prikaz xt_geoip_dl

- `./xt_geoip_dl`

A potom vytvorime GeoIP databazi

- `./xt_geoip_build -D /usr/share/xt_geoip/ *.csv`

```
138540 entries total
    0 IPv6 ranges for A1 Anonymous Proxy
   91 IPv4 ranges for A1 Anonymous Proxy
    0 IPv6 ranges for A2 Satellite Provider
  337 IPv4 ranges for A2 Satellite Provider
    3 IPv6 ranges for AD Andorra
   13 IPv4 ranges for AD Andorra
   46 IPv6 ranges for AE United Arab Emirates
  182 IPv4 ranges for AE United Arab Emirates
   14 IPv6 ranges for AF Afghanistan
   88 IPv4 ranges for AF Afghanistan
...
```

Nyni muzeme v iptables pracovat s databazi IP adres:

- `-A FORWARD -m geoip --src-cc CN -d a.b.c.d/32 -j DROP`

Seznam kodu jednotlivych statu nalezneme napr. zde ve wiki

GeoIP v Debianu 11

```
apt install xtables-addons-common xtables-addons-dkms libtext-csv-xs-perl
```

`libnet-cidr-lite-perl`

```
modprobe xt_geoip
```

Modul pridame take do `/etc/modules-load.d/geoip.conf` `mkdir -p /usr/share/xt_geoip`

```
#!/bin/bash
cd /tmp
/usr/libexec/xtables-addons/xt_geoip_dl
/usr/libexec/xtables-addons/xt_geoip_build -D /usr/share/xt_geoip *.csv
```

- Pokud pouzivame kernel verze 5.x v debianu 11, musime stahnout balicky xtables verze 3.18 z debianu testing (v debianu 11 je verze 3.11, kde nejde kompilovat dkms modul oproti 5.x kernelu

From:
https://wiki.spoje.net/ - **SPOJE.NET**

Permanent link:
https://wiki.spoje.net/doku.php/howto/network/iptables

Last update: **2022/02/09 12:01**