

Ugniasien?

Spėjimas

Šis gidas skirtas žmonėms, kurie turi patirties Linux serverių administravimo srityje. Ugniasienės diegimas gali būti pavojingas. Galite užblokuoti savo serverį ir turėsite jį perkrauti nutraukdami maitinimo tiekimą. Jeigu padarysite klaidą galutiniame scenarijuje, visai negalėsite prisijungti prie savo serverio! Būkite atsargūs ir, jeigu žiūrėsite gide ko nors nesuprasite, nediekite ugniasienės į savo serverį!

Kas yra ugniasienė?

Tai yra programinė įranga, kuri blokuoja tam tikrus įėjimo serverio prievadus. Kad geriau suprastumėte, pavaizduokime namą: jame yra priekinis ir galinis durys. Jeigu niekada nenaudojate galinių durų, galite jas užblokuoti ir taip sumažinti potencialų riziką, kad per jas gali sibrauti vagis. Panašiai vyksta ir su serveriu: uždaromi visi nereikalingi prievadai.

Kurie prievadai dažniausiai naudojami?

Dėmesio!

Prie ką nors darydami būkite labai atsargūs, nes galite uždaryti net prievadą. Pavaizduokite, jeigu uždarysite SSH prievadą, turėsite jungtis telnet ryšiu, naudodami webmin sąsają arba perkrauti serverį.

Pagal nutylėjimą OVH atidaromi serverių prievadai yra:

21 – ftp (FTP serveris). 22 – ssh (šifrui vartotojo prieiga). 23 – telnet (nešifrui vartotojo prieiga). 25 – smtp (SMTP serveris). 53 – dns (DNS serveris). 80 – http (internetinio serverio). 110 – pop3 (pašto priėmimo serveris). 143 – imap (pašto priėiga, jeigu nenaudojamas POP3). 443 – https (šifrui internetinio prieiga). 1000 – webmin (serverio konfigūravimo sąsaja).

Šie prievadai atidaromi pagal nutylėjimą, tačiau tai priklauso nuo diegtos programos rangos: gali būti atidaryti ne visi išvardinti prievadai, gali būti atidaryti ir kiti. Jūs patys sprendiate, kuriuos prievadus palikti atvirus. Kai pasirinksite, galime pradėti.

Iptables

Iptables yra galinga ugniasienė, diegiama visus OVH serverius. Iptables konfigūravimo pavyzdys: atidarysime kai kuriuos prievadus, o likusius uždarysime. Žiūrėkite pavyzdyje paliksime atvirus tik 22 (SSH) ir 80 (HTTP) prievadus. Tai tik pavyzdys, savo serverio ugniasienę konfigūruokite pagal savo poreikius.

```
Prisijunkite per SSH kaip root. Pirmiausiai patikrinkime Iptables versiją: $ /sbin/iptables -V iptables v1.2.4
Versija per seną. Diegsime 1.2.9: $ cd /root $ wget http://www.netfilter.org/files/iptables-1.2.9.tar.bz2 $ tar
xvfj iptables-1.2.9.tar.bz2 $ cd iptables-1.2.9 $ make KERNEL_DIR=/usr/src/linux $ make install
KERNEL_DIR=/usr/src/linux $ cd /sbin $ mv iptables iptables.old $ mv iptables-restore iptables-restore.old
$ mv iptables-save iptables-save.old $ ln -s /usr/local/sbin/iptables iptables $ ln -s
/usr/local/sbin/iptables-restore iptables-restore $ ln -s /usr/local/sbin/iptables-save iptables-save $
/sbin/iptables -V iptables v1.2.9
```

Baigta, iptables atnaujintos, galime tęsti.

Peržiūrime taisykles:

```
$ /sbin/iptables -L Chain INPUT (policy ACCEPT) target prot opt source destination Chain FORWARD (policy ACCEPT) target prot opt source destination Chain OUTPUT (policy ACCEPT) target prot opt source destination
```

Matome 3 grandines: **Input**, **Forward** ir **Output**. Pirmiausiai dirbsime su **Input** grandine (?einan?io srauto). Autorizuosime 22 ir 80 prievadus:

```
$ /sbin/iptables -A INPUT -i eth0 -p tcp --dport 22 -j ACCEPT $ /sbin/iptables -A INPUT -i eth0 -p tcp --dport 80 -j ACCEPT
```

–A INPUT: nustatome **Input** taisykl?. –i eth0: nurodome, kad dirbame tik su ethernet s?saja. –p tcp: nurodome, kad dirbame su TCP protokolu (?iuo metu tik su juo ir dirbsime). --dport 22: taisykl? bus taikoma SSH (22) prievadui. –j ACCEPT: priimsime ?? sraut?.

Per?i?rime taisykles:

```
$ /sbin/iptables -L Chain INPUT (policy ACCEPT) target prot opt source destination ACCEPT tcp ? anywhere anywhere tcp dpt:ssh ACCEPT tcp ? anywhere anywhere tcp dpt:www Chain FORWARD (policy ACCEPT) target prot opt source destination Chain OUTPUT (policy ACCEPT) target prot opt source destination
```

Skyrius **Input** ?iek tiek u?pildytas, tai geras ?enklas ;).

Matome, kad numatytoji taisykl? yra visk? priimti **Chain INPUT(policy ACCEPT)**. Mes norime u?blokuoti vis? nepageidaujam? sraut?. Tod?l ?trauksime taisykl?, kuri u?blokuos visus prievadus. Ta?iau susiduriame su problema:

Pavyzd?iui, j?s? serveris susijings su kernel.org serveriu, kad parsist? nauj? branduol?, tod?l sukurs nauj? jungt? su svetaine, kuri lauks j?s? serverio atsako. Kitaip sakant, u?klausa pasieks kernel.org, ta?iau kaip ji gr??, jeigu mes visk? blokuojame?

Laimei, iptables yra pakankamai galinga programa ir gali atrinkti paketus pagal j? b?sen?. Taigi ?traukiame taisykl?:

```
$ /sbin/iptables -A INPUT -i eth0 -m state --state ESTABLISHED,RELATED -j ACCEPT
```

Dabar galime u?blokuoti visa kita (D?MESIO: toliau ugniasien? prad?s pilnai veikti, ?sitikinkite, kad ?traukiate teisingas taisykles, antraip u?blokuosite savo server?!):

```
$ /sbin/iptables -A INPUT -i eth0 -j DROP
```

?iai taisyklei yra 2 pasirinkimai. Pirmasis sprendimas yra trinti visus nepageidaujamus paketus, t.y. kai b?t? gautas toks paketas, jis b?t? nepriimtas ir i?kart i?trintas. Klientas lauks serverio atsako, kol baigsis u?klausa skirtas laikas. Antrasis pasirinkimas – tai vis? nepageidaujam? paket? atmetimas (vietoje **DROP** naudojama **REJECT** taisykl?). Jeigu gaunamas nelauktas paketas, klientui atgal siun?iamas klaidos prane?imas ir jam nereikia laukti, kol baigsis u?klausa skirtas laikas.

Paket? atmetimas yra ?varesnis metodas, o trynimas – saugesnis. ?sivaizduokite, kad kas nors cikli?kai siun?ia nelauktus paketus ? j?s? server?. Kai paketai i?trinami, serveris tiesiog neapdoros j?, o jeigu paketai atmetami, neigiamo atsakymo siuntimui bus naudojami serverio resursai ir laikas.

J?s patys sprend?iate, kur? metod? naudoti ;)

Nor?dami panaikinti visas ugniasien?s taisykles, ra?ykite:

```
$ /sbin/iptables -F INPUT
```

?? komanda pa?alins visas **Input** dalies taisykles. Jeigu norite ?traukti taisykl? tarp pirmos ir antros, ra?ykite:

```
$ /sbin/iptables -I INPUT 2 ... j?s? taisykl?
Nor?dami i?trinti 3 taisykl?:
```

```
$ /sbin/iptables -D INPUT 3
Nor?dami visi?kai u?blokuoti IP adres?:
```

```
$ /sbin/iptables -I INPUT 1 -s -j DROP
```

Dabar ugniasien? pilnai veikis. Bandykite skanuoti savo server? ir matysite, kad atviri tik 22 ir 80 prievadai. Jeigu skanavimas labai l?tas, vadinasi, naudojama **DROP** taisykl?.

IP adres? autorizavimas ir blokavimas

Jeigu norite u?blokuoti ICMP protokol? (Ping u?klausas), turite praleisti bent **ping.ovh.net**, **proxy.p19.ovh.net**, **proxy.rbx.ovh.net** ir **proxy.ovh.net** u?klausas ? savo server?. Tai leis OVH komandoms steb?ti j?s? serverio busen?.

Tam tikr? IP ir serveri? ICMP u?klaus? praleidimo pavyzdys:

J?s? serverio IP adresas yra aaa.bbb.ccc.ddd Turite praleisti: aaa.bbb.ccc.250 Pavyzd?iui, 213.186.57.153 turi praleisti 213.186.57.250

Jeigu naudojat?s HG serveriu, praleiskite IP aaa.bbb.ccc.249 (laikina taisykl?).

Jeigu u?blokuosite visas PING u?klausas, ?skaitant ir OVH, mes negal?sime tikrinti j?s? serverio b?senos ir, kai atsiras problema, neb?sime apie j? informuoti. Nor?dami praleisti PING u?klausas i? m?s? serveri?, ra?ykite:

```
/sbin/iptables -A INPUT -i eth0 -p icmp --source proxy.ovh.net -j ACCEPT /sbin/iptables -A INPUT -i eth0 -p icmp --source proxy.p19.ovh.net -j ACCEPT /sbin/iptables -A INPUT -i eth0 -p icmp --source proxy.rbx.ovh.net -j ACCEPT /sbin/iptables -A INPUT -i eth0 -p icmp --source ping.ovh.net -j ACCEPT /sbin/iptables -A INPUT -i eth0 -p icmp --source IP.250 -j ACCEPT # IP = aaa.bbb.ccc, pagal ankstesn? taisykl? /sbin/iptables -A INPUT -i eth0 -p icmp --source IP.249 -j ACCEPT # laikinai, tik HG serveriams
```

Kalbant apie SSH, jeigu norite apriboti prieig? tik iki savo IP, rekomenduojame leisti prisijungti ir i? cache.ovh.net. Tokiu atveju, kilus problemoms, mes gal?sime prisijungti prie serverio ir pa?alinti problem?. Jeigu u?darysite 22 prievad? OVH technikams, negal?sime pad?ti, kadangi serveris blokuos m?s? prieig?.

SSH prieig? i? m?s? serverio autorizuosite ?ved? taisykl?:

```
/sbin/iptables -A INPUT -i eth0 -p tcp --dport 22 --source cache.ovh.net -j ACCEPT
```

Jeigu turite RAID pildytoj?, nepamir?kite autorizuoti NFS jung?i?. Mes galime autorizuoti visk?, kas ateina i? vidinio m?s? tinklo 192.168.0.0/16:

```
/sbin/iptables -A INPUT -i eth0 -p tcp --source 192.168.0.0/16 -j ACCEPT /sbin/iptables -A INPUT -i eth0 -p udp --source 192.168.0.0/16 -j ACCEPT
```

Jeigu naudojate serveri? grup?s konfig?racij?, turite atidaryti 79 prievad?, kad OCO susijungt? su apkrovos skirstytuvu.

```
/sbin/iptables -A INPUT -i eth0 -p tcp --dport 79 -j ACCEPT
```

Pilnos konfig?racijos pavyzdys

Toliau pateikiamas pilnas scenarijus, skirtas apsaugoti server? su Iptables. Tai n?ra b?tina, kadangi visos j?s? serverio paslaugos ir taip pasiekiamos, ta?iau vis tiek galite naudoti sav?j? konfig?racij?:

```
/sbin/iptables -A INPUT -i eth0 -m state --state ESTABLISHED,RELATED -j ACCEPT /sbin/iptables -A INPUT -i eth0 -p tcp --dport 25 -j ACCEPT /sbin/iptables -A INPUT -i eth0 -p tcp --dport 53 -j ACCEPT /sbin/iptables -A INPUT -i eth0 -p udp --dport 53 -j ACCEPT /sbin/iptables -A INPUT -i eth0 -p tcp --dport 80 -j ACCEPT /sbin/iptables -A INPUT -i eth0 -p tcp --dport 110 -j ACCEPT /sbin/iptables -A INPUT -i eth0 -p tcp --dport 443 -j ACCEPT /sbin/iptables -A INPUT -i eth0 -p tcp --dport 10000 -j ACCEPT /sbin/iptables -A INPUT -i eth0 -p tcp --dport 21 --source xx.xx.xx.xx -j ACCEPT /sbin/iptables -A INPUT -i eth0 -p tcp --dport 22 --source cache.ovh.net -j ACCEPT /sbin/iptables -A INPUT -i eth0 -p tcp --dport 22 --source xx.xx.xx.xx -j ACCEPT /sbin/iptables -A INPUT -i eth0 -p icmp --source proxy.ovh.net -j ACCEPT /sbin/iptables -A INPUT -i eth0 -p icmp --source proxy.p19.ovh.net -j ACCEPT /sbin/iptables -A INPUT -i eth0 -p icmp --source proxy.rbx.ovh.net -j ACCEPT /sbin/iptables -A INPUT -i eth0 -p icmp --source ping.ovh.net -j ACCEPT /sbin/iptables -A INPUT -i eth0 -p tcp --source 192.168.0.0/16 -j ACCEPT /sbin/iptables -A INPUT -i eth0 -p udp --source 192.168.0.0/16 -j ACCEPT /sbin/iptables -A INPUT -i eth0 -p tcp --dport 79 -j ACCEPT /sbin/iptables -A INPUT -i eth0 -j REJECT
```

?iose taisykl?se pakeiskite xx.xx.xx.xx atitinkamai IP adresais.

Ugniasien?s automatizavimas

Kai gerai sukongfig?ruosite savo ugniasien?, gal?site sukurti scenarij?, kuris bus vykdomas kiekvieno serverio ?krovimo metu. Toliau pateikiamas pavyzdys, kaip i?saugoti fail?, pavadinimu "firewall", kataloge /etc/init.d/:

```
#!/bin/sh 1. chkconfig: 3 21 91 2. description: Firewall IPT=/sbin/iptables case "$1" in start) $IPT -A INPUT -i eth0 -m state --state ESTABLISHED,RELATED -j ACCEPT $IPT -A INPUT -i eth0 -p tcp --dport 25 -j ACCEPT $IPT -A INPUT -i eth0 -p tcp --dport 53 -j ACCEPT $IPT -A INPUT -i eth0 -p udp --dport 53 -j ACCEPT $IPT -A INPUT -i eth0 -p tcp --dport 80 -j ACCEPT $IPT -A INPUT -i eth0 -p tcp --dport 110 -j ACCEPT $IPT -A INPUT -i eth0 -p tcp --dport 443 -j ACCEPT $IPT -A INPUT -i eth0 -p tcp --dport 10000 -j ACCEPT $IPT -A INPUT -i eth0 -p tcp --dport 21 --source xx.xx.xx.xx -j ACCEPT $IPT -A INPUT -i eth0 -p tcp --dport 22 --source cache.ovh.net -j ACCEPT $IPT -A INPUT -i eth0 -p tcp --dport 22 --source xx.xx.xx.xx -j ACCEPT $IPT -A INPUT -i eth0 -p icmp --source proxy.ovh.net -j ACCEPT $IPT -A INPUT -i eth0 -p icmp --source proxy.p19.ovh.net -j ACCEPT $IPT -A INPUT -i eth0 -p icmp --source proxy.rbx.ovh.net -j ACCEPT $IPT -A INPUT -i eth0 -p icmp --source ping.ovh.net -j ACCEPT $IPT -A INPUT -i eth0 -p tcp --source 192.168.0.0/16 -j ACCEPT $IPT -A INPUT -i eth0 -p udp --source 192.168.0.0/16 -j ACCEPT $IPT -A INPUT -i eth0 -p tcp --dport 79 -j ACCEPT $IPT -A INPUT -i eth0 -j REJECT exit 0 ;; stop) $IPT -F INPUT exit 0 ;; *) echo "Usage: /etc/init.d/firewall {start|stop}" exit 1 ;; esac
```

Suteikite 700 teises ir ?vykdykite komand? "/etc/init.d/firewall start", kad paleistum?te ugniasien? ir "/etc/init.d/firewall stop", kad j? i?jungtum?te. Jeigu norite, kad ugniasien? automati?kai pasileist? kiekvieno ?krovimo metu:

```
$ /sbin/chkconfig --level 3 firewall on $ /sbin/chkconfig --level 06 firewall off
```

Prie? nustatydami scenarijaus paleidim? kiekvieno krovimo metu ?sitikinkite, kad jis sukurs teising? konfig?racij?, antraip galite visi?kai u?blokuoti prieig? prie savo serverio!