Linux videot: <https://www.youtube.com/playlist?list=PLZw_fXxI6L50ovlxunMvWw-bEDc3TiBQp>

Contents

[Iptables 1](#_Toc51226888)

[Esimerkkitehtävä 1](#_Toc51226889)

[Mitä portteja palvelu käyttää? 2](#_Toc51226890)

[Tallentaminen 2](#_Toc51226891)

[PING salliminen 2](#_Toc51226892)

[Sääntöjen poistaminen 3](#_Toc51226893)

Iptables on Linuxin palomuuri, jolla saa aikaan yksinkertaisia ja monimutkaisia asetuksia, joilla voidaan suojata palvelimen palveluita.

# Iptables

Asennetaan iptables paketti:

**sudo apt install iptables**

Asenna myös seuraava paketti, jotta iptables tehdyt asetukset säilyvät uudelleenkäynnistyksen jälkeen.

**sudo apt install iptables-persistent**

# Esimerkkitehtävä

Esimerkkitehtävä Taitaja2018 Linux semifinaali tehtävästä:



Aluksi kaikki palvelimelle TULEVAT yhteydet tulee estää:

**iptables -P INPUT DROP**

Tässä vaiheessa voit testata esim. että SSH ja http yhteydet eivät toimi.

Sitten sallitaan yksitellen eri protokollat jotka halutaan sallia:

**iptables -A INPUT -p tcp --dport 22 -j ACCEPT**

**iptables -A INPUT -p tcp --dport 80 -j ACCEPT**

**iptables -A INPUT -p tcp --dport 443 -j ACCEPT**

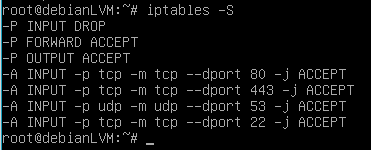
**iptables -A INPUT -p udp --dport 53 -j ACCEPT**

HUOM! ennen dport kohtaa on kaksi väliviiva - merkkiä eli --

HUOM! Ensimmäiset kolme porttia (SSH, http ja HTTPS) toimivat TCP protokollalla, mutta viimeinen portti (DNS) toimii UDP protokollalla.

Säännöt näyttäisivät tältä:

**iptables -S**



## Mitä portteja palvelu käyttää?

Saat selville mitä portteja eri palvelut käyttävät etsimällä tietoa netistä.

Esimerkki hakutermistä:

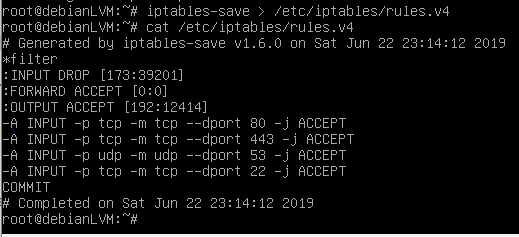
**samba network ports**

# Tallentaminen

Tallenna säännöt (varmista myös, että iptables-persistent paketti on asennettuna):

**iptables-save > /etc/iptables/rules.v4**

/etc/iptables/rules.v4 on siis periaatteessa iptables konfiguraatio tiedosto, johon iptables-save tiedot välitetään > merkkiä hyväksikäyttäen.



# PING salliminen

Jos kaikki yhteydet on estetty, myös palvelimen pingaaminen ei toimi.

HUOM! ennen icmp-type kohtaa on kaksi väliviivaa - merkkiä eli --

Sen voi sallia seuraavasti:

**iptables -A INPUT -p icmp --icmp-type 8 -j ACCEPT**

# Sääntöjen poistaminen

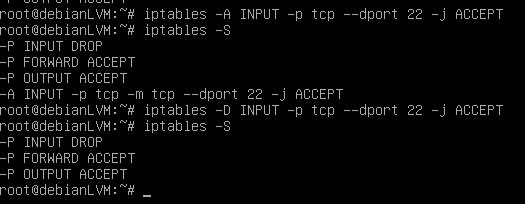
Tehtyjä palomuuri sääntöjä voi poistaa -D parametrilla. Tässä esimerkissä sallitaan SSH yhteys, eli portti 22.

Sääntö luodaan -A parametrilla:

**iptables -A INPUT -p tcp --dport 22 -j ACCEPT**

Sääntö poistetaan -D parametrilla:

**iptables -D INPUT -p tcp --dport 22 -j ACCEPT**



# Iptables asennus ja conffaus

Tehnyt: Aleksi Sievälä

Komento, jolla näkee tehdyt conffaukset:

**sudo iptables -L -v**

Voit luoda muokata kolmen eri kulkutavan oikeuksia:

**INPUT –** Tietokoneelle saapuvat paketit

**FORWARD –** Tietokoneelle saapuvat paketit, jotka ovat jatkamassa matkaa vielä tietokoneelta eteenpäin

**OUTPUT –** Tietokoneelta lähtevät paketit

Voit asettaa iptablesille kolme eri tapaa hoitaa paketit:

**ACCEPT –** Hyväksytään pakettien saapuminen tietokoneelle

**DROP –** Hylätään saapuvat paketit

**RETURN –** Hylätään tämänhetkinen tapa ja palataan seuraavaan tapaan

Esim. hyväksytään https pyynnöt ja hylätään http pyynnöt:

**sudo iptables -A INPUT -p tcp --dport 443 -j ACCEPT**

**sudo iptables -A INPUT -p tcp --dport 80 -j DROP**

Tässä tapauksessa **-A,** tarkoittaa “append” ja **-p** tarkoittaa ”protocol”, lisää tietoja löytyy **sudo iptables -h** komennolla.

Jos tiettyä porttia halutaan muuttaa tietylle verkolle tai ip-osoitteelle, käytetään seuraavaa komentoa (korvaa 10.3.57.x omalla osoitteella):

**1 ip-osoite:**

**sudo iptables -A INPUT -p tcp -s 10.3.57.100 --dport -j ACCEPT**

**Verkko:**

**sudo iptables -A INPUT -p tcp -s 10.3.57.0/24 --dport -j ACCEPT**

Voit jättää kaiken liikenteen paitsi erikseen asetetut komennolla:

**sudo iptables -A INPUT -j DROP**

Asetuksia voi tallentaa seuraavalla tavalla:

**iptables-save > /etc/iptables/rules.v4**