iptables: ftp

- Ftp on palomuureille vaikea protokolla, koska siinä on erotettu ohjaus ja datansiirto eri portteihin ja porttineuvottelut käydään palomuurin näkökulmasta siirrettävän datan sisällä. Sillä on lisäksi kaksi erilaista toimintatapaa, aktiivinen ja passiivinen:
  - Aktiivinen ftp: palvelin avaa datayhteyden asiakkaan ilmoittamaan porttiin.
  - Passiivinen ftp: asiakas avaa datayhteyden palvelimen ilmoittamaan porttiin.
  - Siis joko asiakkaan tai palvelimen sekä välissä olevien palomuurien pitää sallia yhteys uuteen, satunnaiseen porttiin.

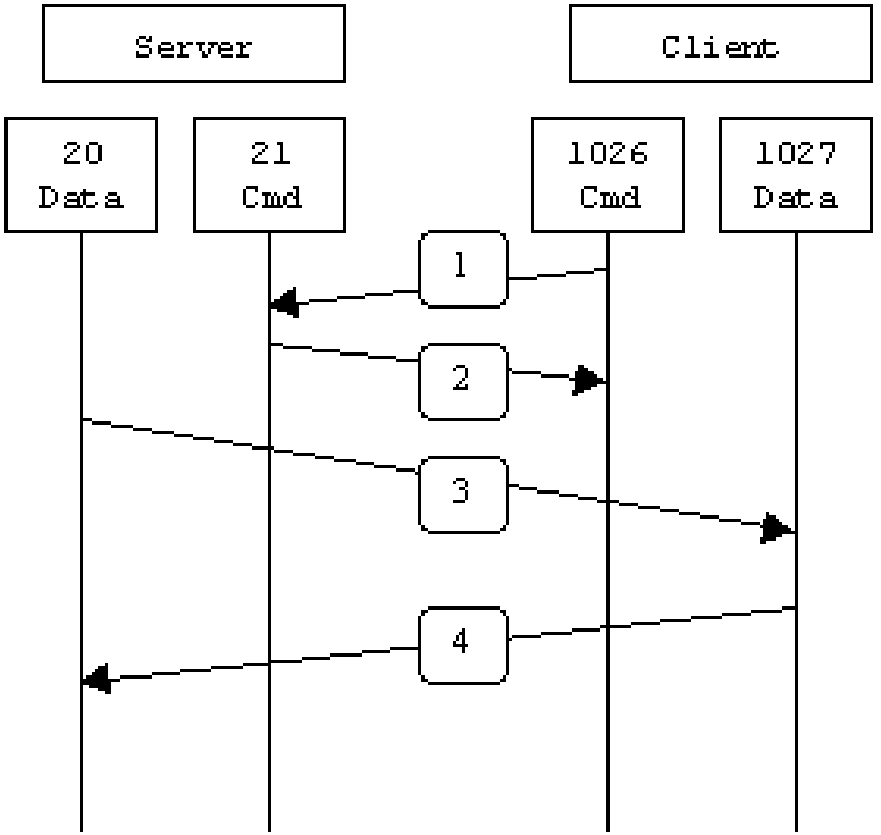
iptables: ftp

- Sekä aktiivisessa että passiivisessa ftp:ssä ensimmäinen, kontrolliyhteys avataan samalla tavalla: asiakas ottaa yhteyden palvelimen porttiin 21. Palvelin vastaa normaaliin tapaan, palomuurit osaavat sallia tämän "established" -liikenteenä.
- Dataliikennettä varten käytettävää porttia palomuuri ei tunnista ilman erillistä helper-modulia yhteydenseurannan avuksi (moduli nf_conntrack_ftp, aiemmin ip_conntrack_ftp). Aikaisemmin se piti ladata modprobe-komennolla tms, nykyisin iptables osaa yleensä hoitaa asian itse (--helper ftp).
- Helper-modulille pitää kertoa mitä porttia sen pitää seurata erillisellä säännöllä raw-taulussa (ketju PREROUTING tai OUTPUT).

Aktiivinen ftp

- Aktiivinen ftp toimii porttitasolla näin:
- Asiakas ottaa yhteyden palvelimen porttiin 21, source port jotain 1024-65535 (esim. 1026) ja ilmoittaa sille haluamansa portin datayhteydelle (yleensä kontrolliyhteyden sport+1, esim. 1027).
- Palvelin ottaa yhteyden asiakkaan ilmoittamaan porttiin (palvelimen source port 20), asiakas vastaa (sport 1027, dport 20).
- Asiakkaan pitää siis sallia palvelimen yhteydenotot omaan (vaihtuvaan) porttiinsa.
- Kontrolli (komennot) kulkee sen jälkeen normaaliin tapaan palvelimen portista 21, data portista 20.

Aktiivinen ftp

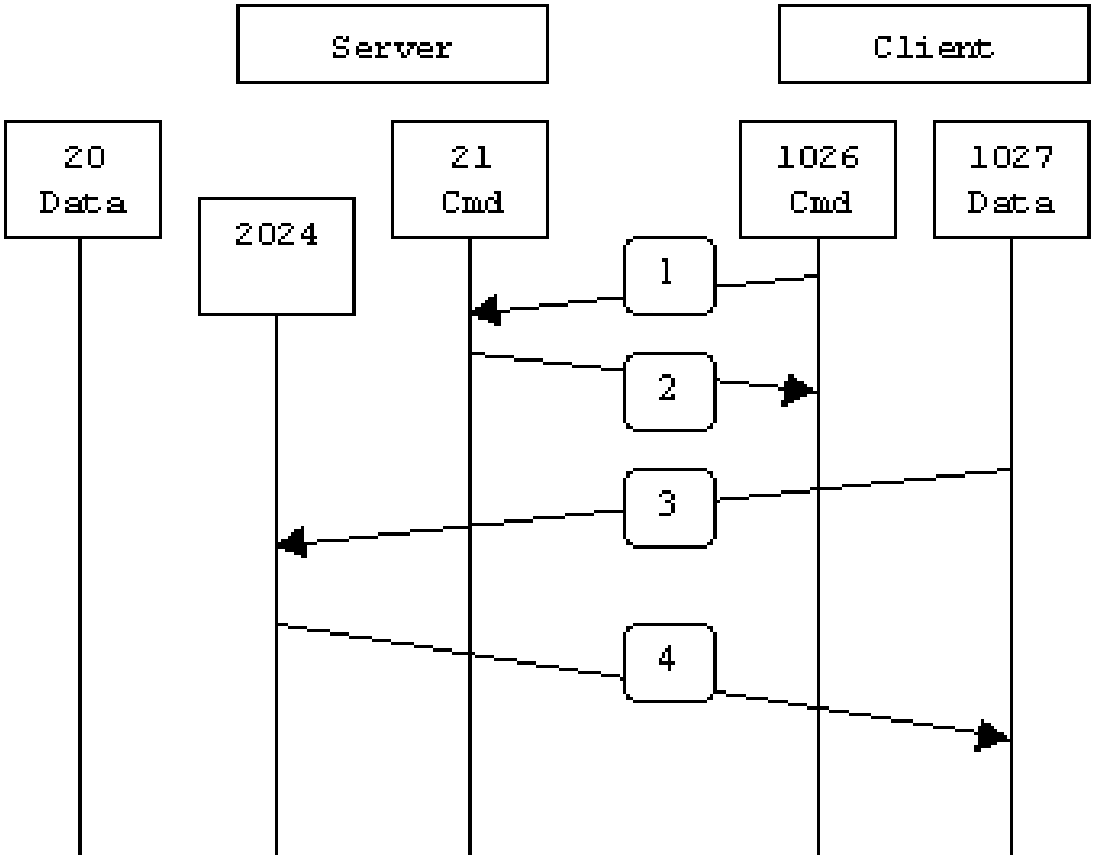


http://slacksite.com/other/ftp.html

Passiivinen ftp

- Passiivinen ftp toimii porttitasolla näin:
- Asiakas ottaa (ohjaus)yhteyden ftp-palvelimen porttiin 21 ja ilmoittaa haluavansa passiivisen yhteyden.
- Palvelin ilmoittaa asiakkaalle valitsemansa (satunnaisen) portin (esim. 2024) datayhteyttä varten.
- Asiakas ottaa yhteyden palvelimen ilmoittamaan porttiin.
- Asiakkaan tarvitsee sallia sisään vain paluuliikenne.
- Data siirtyy edellä valitun portin kautta, ohjauskomennot taas portin 21 kautta.

Passiivinen ftp



http://slacksite.com/other/ftp.html

iptables: ftp server

- Passiivinen ftp käyttää oletuksena satunnaisia portteja väliltä 1024-65535. Palomuurin säätö helpottuu jos niitä rajataan palvelimella, esim. /etc/vsftpd.conf'issa tähän tapaan:

  pasv_min_port=50020

  pasv_max_port=50040

  Porttialue kannattaa yleensä valita väliltä 49152-65535 (IANAn "private/ephemeral" portit), määrä rajoittaa yhtaikaisten yhteyksien määrää (mikä voi olla haluttuakin, pieni määrä myös helpottaa palomuurien toimintaa).
- Palvelimen saa toimimaan ilman conntrack-moduliakin hieman turvattomasti avaamalla portteja enemmän kuin oikeasti tarvitaan.

iptables: ftp server

- FTP palvelin, turvattomat säännöt ilmani yhteydenseurantamodulia

  # ftp control

  -A input -p tcp --dport 21 -m state --state NEW,ESTABLISHED -j ACCEPT

  -A output -p tcp --sport 21 -m state --state ESTABLISHED -j ACCEPT

  # active ftp

  # sallitaan uudetkin yhteydet ulos portista 20 kaikkiin portteihin

  # ilman yhteydenseurantaa ei voi erottaa uudesta

  -A output -p tcp --sport 20 --dport 1024: -j ACCEPT

  -A input -p tcp --dport 20 -m state --state ESTABLISHED -j ACCEPT

  # passive ftp (portit rajattu /etc/vsftpd.conf'issa tms; ellei, 1024: toimii)

  # sallitaan uudetkin yhteydet sisään

  -A input -p tcp --dport 50020:50040 -j ACCEPT

  -A output -p tcp --sport 50020:50040 -m state --state ESTABLISHED -j ACCEPT

iptables: ftp server

- FTP palvelin, tiukat säännöt yhteyden seurannalla

  # ohjataan portti 21 ftp helper modulille

  -t raw -A PREROUTING -p tcp --dport 21 -j CT --helper ftp

  # ftp control

  -A INPUT -p tcp --dport 21 -m state --state NEW,ESTABLISHED -j ACCEPT

  -A OUTPUT -p tcp --sport 21 -m state --state ESTABLISHED -j ACCEPT

  # active ftp: vain related ja established ulos, vain established sisään

  -A OUTPUT -p tcp --sport 20 -m state --state RELATED,ESTABLISHED -j ACCEPT

  -A INPUT -p tcp --dport 20 -m state --state ESTABLISHED -j ACCEPT

  # passive ftp: vain related ja established sisään, vain established ulos

  -A INPUT -p tcp --dport 50020:50040 -m state --state RELATED,ESTABLISHED -j ACCEPT

  -A OUTPUT -p tcp --sport 50020:50040 -m state --state ESTABLISHED -j ACCEPT

iptables: ftp client

- Ftp saattaa tarvita client-päässäkin palomuurin säätöä. Tyypillisillä "kaikki ulospäin ja paluuliikenne takaisin" -säännöillä passiivinen ftp toimii suoraan, mutta jos liikennettä ulospäinkin on rajoitettu tai jos halutaan käyttää aktiivista ftp:tä, client-päässä tarvitaan olennaisesti vastaavat säädöt kuin serverissäkin, ikäänkuin niiden peilikuvina vain.
- Tässä tapauksessa ftp helper -sääntö pitää laittaa OUTPUT-ketjuun, lähtevässä liikenteessä raw-taulu on siellä.
- Palvelimen käyttämää porttialuetta passiivisessa ftp:ssä ei asiakas kuitenkaan yleensä voi tietää, joten sille pitää sallia kaikki portit, tai ainakin 1024-65535.

iptables: ftp client

- FTP client, tiukat säännöt yhteyden seurannalla

  # porttiin 21 uloslähtevä liikenne ftp helper -modulille

  -t raw -A OUTPUT -p tcp --dport 21 -j CT --helper ftp

  # ftp control

  -A OUTPUT -p tcp --dport 21 -m state --state NEW,ESTABLISHED -j ACCEPT

  -A INPUT -p tcp --sport 21 -m state --state ESTABLISHED -j ACCEPT

  # active ftp

  -A INPUT -p tcp --sport 20 -m state --state RELATED,ESTABLISHED -j ACCEPT

  -A OUTPUT -p tcp --dport 20 -m state --state ESTABLISHED -j ACCEPT

  # passive ftp

  -A OUTPUT -p tcp --dport 1024: -m state --state RELATED,ESTABLISHED -j ACCEPT

  -A INPUT -p tcp --sport 1024: -m state --state ESTABLISHED -j ACCEPT

iptables: ftp reitittimessä

- Ftp-liikenteen päästäminen reitittimenä toimivan palomuurin läpi tarvitsee vielä hieman erilaiset säännöt.
- Jos palomuuri myös NATtaa liikenteen ftp-palvelimelle, esimerkiksi jos ftp-palvelin on virtuaalikone ja alustakone toimii palomuurina, myös NAT-sääntöjä pitää säätää ftp:tä varten (tyypillisesti PREROUTING DNAT).
- Seuraavassa esimerkissä palomuurin ulkoinen verkkortti on eth0 ja sisäinen eth1, palomuurin sisäpuolella olevan ftp-palvelimen (sisäinen) osoite 10.1.1.1, reitityssääntöjä ei ole näytetty.
- Tämän esimerkin säännöt eivät salli yhteyttä itse palomuurista ftp-palvelimeen eivätkä yhteyksiä palomuurin takana olevasta asiakkaasta palvelimeen sen ulkopuolella.

iptables: ftp reitittimessä

ftp helper helper sisääntulevalle (välitettävälle) liikenteelle porttiin 21

-t raw -A PREROUTING -p tcp --dport 21 -j CT --helper ftp

ftp control

-A FORWARD -i eth0 -o eth1 -d 10.1.1.1 -p tcp -m tcp --dport 21 -m state --state NEW,ESTABLISHED -j ACCEPT

-A FORWARD -i eth1 -o eth0 -s 10.1.1.1 -p tcp -m tcp --sport 21 -m state --state ESTABLISHED -j ACCEPT

passive ftp

-A FORWARD -i eth0 -o eth1 -d 10.1.1.1 -p tcp -m tcp --dport 50020:50040 -m state --state RELATED,ESTABLISHED -j ACCEPT

-A FORWARD -i eth1 -o eth0 -s 10.1.1.1 -p tcp -m tcp --sport 50020:50040 -m state --state ESTABLISHED -j ACCEPT

active ftp

-A FORWARD -i eth0 -o eth1 -d 10.1.1.1 -p tcp -m tcp --dport 20 -m state --state ESTABLISHED -j ACCEPT

-A FORWARD -i eth1 -o eth0 -s 10.1.1.1 -p tcp -m tcp --sport 20 -m state --state RELATED,ESTABLISHED -j ACCEPT

NFS: Network File System

- Keino jakaa tiedostojärjestelmä kokonaan tai osittain (alihakemisto) toiselle koneelle.
- NFSv3:ssa *koneet* luottavat toisiinsa, vähänlaisesti tietoturvaominaisuuksia.

  NFSv4 lisää paljon mm. käyttäjäkohtaisen autentikoinnin ja kaikenlaista muutakin.

  Seuraavissa esimerkeissä NFSv3 ellei toisin mainita.

NFS: Network File System

- **Palvelimella** (tunnus2): apt-get install nfs-kernel-server

  /etc/exports:

  /home tunnus1(rw,sync,no_subtree_check,root_squash)

  exportfs -a

  jos virhe ”... not implemented”:

  systemctl restart nfs-mountd

  (vanhemmssa Ubuntuissa service nfs-kernel-server restart)

  Ks. /etc/default/nfs-kernel-server

NFS: Network File System

- Yleisiä optioita /etc/exports'issa (ks. man 5 exports):

rw	read+write (oletus readonly)
async	nopea, vaarallinen jos palvelin kaatuu tms
subtree_check	ekstratarkistuksia jos alihakemisto exportattu
[no_]root_squash	root → nobody (oletuksena päällä)
all_squash	kaikki → nobody (oletuksena pois)

NFS: Network File System

- **Asiakaskoneessa** (tunnus1):

  apt-get install nfs-common

  mkdir /home2; mount tunnus2:/home /home2

  /etc/fstab:

  tunnus2:/home /home2 nfs defaults 0 0

  Ks. /etc/default/nfs-common

iptables: NFS

- NFS:n toiminta edellyttää isoa joukkoa erillisiä palveluita, jotka tarvitsevat omat porttinsa auki palomuurissa. Asiaa vaikeuttaa se, että osa niistä arpoo portin satunnaisesti, ellei sitä erikseen kiinnitä. Tarvittavat palvelut ovat (suluissa portti jos se on kiinteä): portmapper (111), nfsd (2049), lockd, mountd ja statd, sekä levykiintiöitä käytettäessä rquotad. NFSv4 käyttää vielä yhtä ns. callback-porttia.
- Portit on helppo kiinnittää palvelimella ja yleensä asiakkaat ovat tiedossa ja omassa hallinnassa, joten niihinkin voi tehdä palomuurisäännöt kiinteillä porttinumeroilla.

iptables: NFS

- Muuttuvat portit voidaan palvelimessa kiinnittää näin:

  statd tiedostossa /etc/default/nfs-common:

  ```
  STATDOPTS="--port 4000 --outgoing-port 4001"
  ```

  mountd tiedostossa /etc/default/nfs-kernel-server:

  ```
  RPCMOUNTDOPTS="--manage-gids --port 4002"
  ```

  lockd ja (NFSv4) callback tiedostossa (esim.) /etc/modprobe.d/lockd.conf:

  ```
  options lockd nlm_udpport=4003 nlm_tcpport=4003
  options nfs callback_tcpport=4004
  ```

  rquotad tiedostossa /etc/defaults/quota:

  ```
  RPCRQUOTADOPTS="-p 4005"
  ```

iptables: NFS

- Portit pitää sitten avata palvelimen palomuurissa esim. näin:

  iptables -A INPUT -p tcp -m multiport --dports 111,2049,4000:4005 -j ACCEPT

  iptables -A INPUT -p udp -m multipors --dports 111,2049,4000:4005 -j ACCEPT

  iptables -A OUTPUT -p tcp -m multiport --sports 111,2049,4000:4005 -m state --state ESTABLISHED -j ACCEPT

  iptables -A OUTPUT -p udp -m multiport --sports 111,2049,4000:4005 -m state --state ESTABLISHED -j ACCEPT

  ja vastaavat säännöt asiakkaisiin (INPUT ja OUTPUT päinvastoin) ja mahdolliseen välissä olevaan palomuuriin FORWARDit.

- Valitut portit kannattaa lisätä tiedostoon /etc/services.

iptables: NFS

- /etc/services NFS:ää varten (esimerkki)

```
sunrpc          111/tcp         portmapper      # RPC 4.0 portmapper
sunrpc          111/udp         portmapper
nfs             2049/tcp                        # Network File System
nfs             2049/udp                        # Network File System
rpc.statd-bc    4000/tcp                        # RPC statd broadcast
rpc.statd-bc    4000/udp                        # RPC statd broadcast
rpc.statd       4001/tcp                        # RPC statd listen
rpc.statd       4001/udp                        # RPC statd listen
rpc.mountd      4002/tcp                        # RPC mountd
rpc.mountd      4002/udp                        # RPC mountd
rcp.lockd       4003/tcp                        # RPC lockd/nlockmgr
rcp.lockd       4003/udp                        # RPC lockd/nlockmgr
nfs.callback    4004/tcp                        # NFSv4 callback
rpc.quotad      4005/tcp                        # RPC quotad
rpc.quotad      4005/udp                        # RPC quotad
```

Automounter (autofs)

- mounttaa nfs- tai muita (verkko)levyjä (myös CD:tä yms) tarpeen mukaan, ja umounttaa kun tarve poistuu
- asennus: apt-get install autofs
- mounttauksesta huolehtii demoni automount
- konfiguraatiotiedostot: /etc/auto.master ja siellä viitatut ns. kuvaustiedostot, map files (useimmiten /etc/auto.jotakin)

Automounter (autofs)

- suorat kuvaukset (direct maps): absoluuttinen polku kuvaustiedostossa, harvoin käytetty
- epäsuorat kuvaukset (indirect maps): kuvaustiedostossa suhteellinen polku, yhdistetään master-tiedoston polkumäärityksen
- säätömahdollisuuksia monimutkaisempiin ympäristöihin (LDAP jne)

autofs: esimerkki

- /etc/auto.master:

  /koti /etc/auto.koti --timeout=60

  /- /etc/auto.suora --timeout=180

- /etc/auto.koti:

  oma kotiserver:/home

  naapuri tulppu:/home

autofs: esimerkki

- /etc/auto.suora:

  /jako/peli peliserver:/pelijako

- Näkyvät hakemistot:

  /koti/oma /koti/naapuri /jako/peli

autofs: yleistä

- automountatut hakemistot tulevat näkyviin kun niitä käytetään; edellisessä esimerkissä komento “ls /koti” voi näyttää tyhjää, mutta “cd /koti/oma/tt” toimii kuitenkin (ja sen jälkeen ls toimii myös).
- automounter luo tarvittavat välihakemistot (edellä /koti jne) itse, niitä ei saa tehdä valmiiksi. Niitä ei myöskään saa käyttää muuhun itse.
- master-tiedoston muuttamisen jälkeen tarvitaan

  systemctl reload autofs # tai service autofs reload

autofs: yleistä

- umount tapahtuu automaattisesti määräajan (oletus 5min) kuluttua siitä kun hakemistoja on viimeksi käytetty (tarvittaessa fuser tai lsof tai ps auttavat selvittämään käyttäjän)
- oletusasetukset tiedostossa /etc/default/autofs
- aikoja voi myös muuttaa polkukohtaisesti auto.master -tiedostossa optiolla --timeout (sekunteja)

autofs: wildcards, scripts

- kuvaustiedostossa voi käyttää hakemistonimessä jokerimerkkejä * ja &:
  - kotipalvelin:/home/&
- kuvaustiedosto voi olla skripti, joka tavalla tai toisella tuottaa halutun mounttikuvauksen (argumenttina levypalvelimen nimi); esimerkkinä /etc/auto.net, joka mounttaa mitä vain verkosta löytyy polkuun /net/kone/hakemisto

autofs: debugging

- debuggausta varten automount-demonia voi ajaa verbose-optiolla etualalla omassa ikkunassaan:

```
service autofs stop
/usr/bin/automount -f -v
```

iptables: limit

- Testillä --limit voidaan rajoittaa tietynlaisen liikenteen määrää:

  ... -m limit --limit *n/aikayksikkö* [--limit-burst *m*]

  Optio --limit rajoittaa pakettien määrän per aikayksikkö (second, minute, hour, day) ja --limit-burst kuinka monta pakettia saa ensin tulla peräkkäin ennen kuin niitä aletaan rajoittaa.

- Esim. sallitaan vain 5 ssh-yhteyttä peräkkäin ja sitten 3/minuutti:

  ... -p tcp --dport 22 -m limit --limit 3/minute --limit-burst 5 -j ACCEPT

iptables: limit

- Esimerkki: estetään lokin täyttyminen, esim.

  -N LognDrop

  -A LognDrop -m limit --limit-burst 5 --limit 2/min -j LOG --log-prefix ”evil packet”

  -A LognDrop -j DROP

- Käytettävissä on myös --hashlimit, jolla voidaan tehdä monimutkaisempia rajoituksia tyyliin ”enintään 100 yhteydenottoa per portti-ja-palvelin” jne.

iptables: connlimit

- connlimit -ehdolla voidaan rajoittaa yhtaikaisten yhteyksien määrää, esim.

  ... -p tcp --syn --dport 80 -m connlimit --connlimit-above 20 --connlimit-mask 32 -j DROP

  rajoittaa porttiin 80 (http) samasta osoitteesta tulevien samanaikaisten yhteyksien määrän 20:een. Jos halutaan tehdä vastaava rajoitus yhteydenottajan aliverkolle, se voidaan tehdä --connlimit-mask -optiolla. Optio --syn rajaa testin uusiin yhteydenottoihin.

iptables: recent

- recent -ehdolla voidaan virittää aikaisemmista tapahtumista riippuvia ehtoja. Esimerkiksi ssh-massahyökkäysten torjunta:

  iptables -N SshTest # tehdään uusi ketju

  # kutsutaan ketjua aina kun joku kolkuttaa ssh-porttia

  iptables -A INPUT -i eth0 -p tcp -m tcp --dport 22 -m state --state NEW -j SshTest

  # --set tallettaa tapahtuman joukkoon ”Ssh”

  iptables -A SshTest -m recent --set --name Ssh --rsource

iptables: recent

jos yli 5 yritystä 10 minuutissa, lokitetaan ...

iptables -A SshTest -m recent --update --seconds 600 --hitcount 5 --name Ssh --rsource -j LOG --log-prefix "ssh-attack" --log-level warn

ja blokataan ne

iptables -A SshTest -m recent --update --seconds 600 --hitcount 5 --name Ssh --rsource -j DROP

muussa tapauksessa hyväksytään

iptables -A SshTest -j ACCEPT

Preseeding

- Tehtäessä useita samantapaisia asennuksia voi asennusohjelman kysymysten vastaukset laittaa valmiiksi tiedostoon **preseed.cfg** ja lisätä virt-install'in optioihin

  --initrd-inject preseed.cfg

  Huom. tiedostonimeä ei saa vaihtaa!
- preseed.cfg:n voi myös laittaa CD imageen tms (toimii myös muissa kuin virtuaalikoneasennuksissa)
- Tiedoston preseed.cfg syntaksi on hankala ja tarvittavat asetukset vaihtelevat käyttöjärjestelmäversiosta toiseen, mutta netistä löytyy pohja: https://help.ubuntu.com/lts/installation-guide/example-preseed.txt

  ja vastauksia voi katsoa toimivasta asennuksesta komennoilla

  sudo debconf-get-selections --installer

  sudo debconf-get-selections

  Komento debconf-get-selections löytyy paketista debconf-utils.