IT KOLLEDŽ
TALLINNA TEHNIKAÜLIKOOL

Tulemüür

Operatsioonisüsteemid ja nende haldamine ICA0001

Edmund Laugasson

edmund.laugasson@itcollege.ee

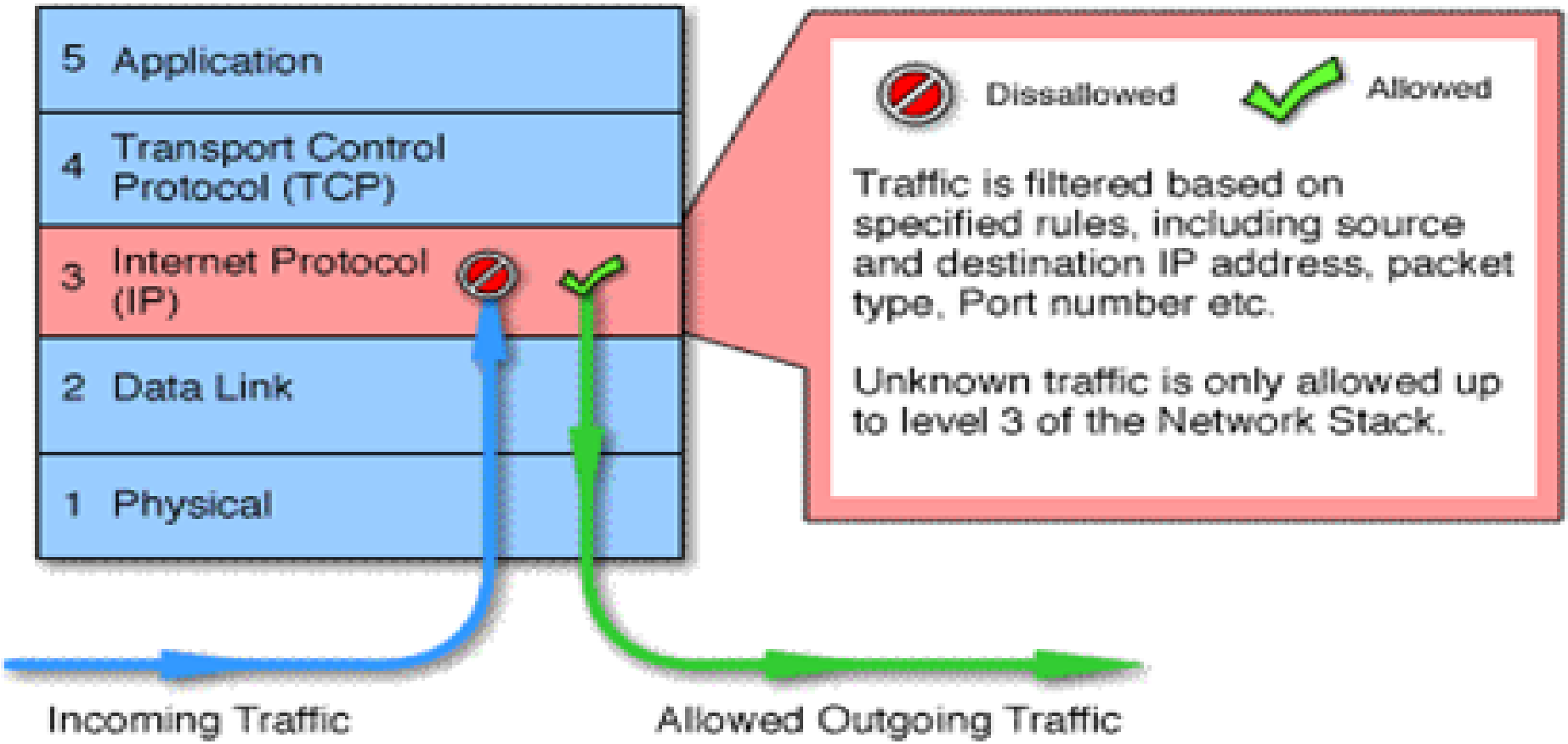
https://wiki.itcollege.ee/index.php/User:Edmund#eesti_keeles

Tulemüürid

- Tulemüürid võib tinglikult jagada kaheks
  - IP pakette filtreerivad tulemüürid (*packet filter*)
    - Teevad otsuseid IP paketi päiseinfo alusel (Näiteks lähte/siht aadressi/pordi alusel)
  - Rakenduspõhised tulemüürid (*application-layer firewall*)
    - Teevad otsuseid paketi sisu alusel (Näiteks ei lubata MS Exchange e-postiserveri suunas suvalisi RPC funktsioonide väljakutseid vaid neid, mida on teenuse kasutamiseks vaja)
  - veel eristatakse võrgutulemüüre (*network firewall*) kahe või enama võrgu (*internet*, *intranet*) liikluse filtreerimiseks ja arvutipõhised tulemüürid (*host-based firewall*) ühe konkreetse arvuti võrguliikluse filtreerimiseks
  - Antud loengus tuleb juttu IP pakettide filtreerimisest ehk tulemüürindusest Linux süsteemides (võrgus)

Tulemüürid

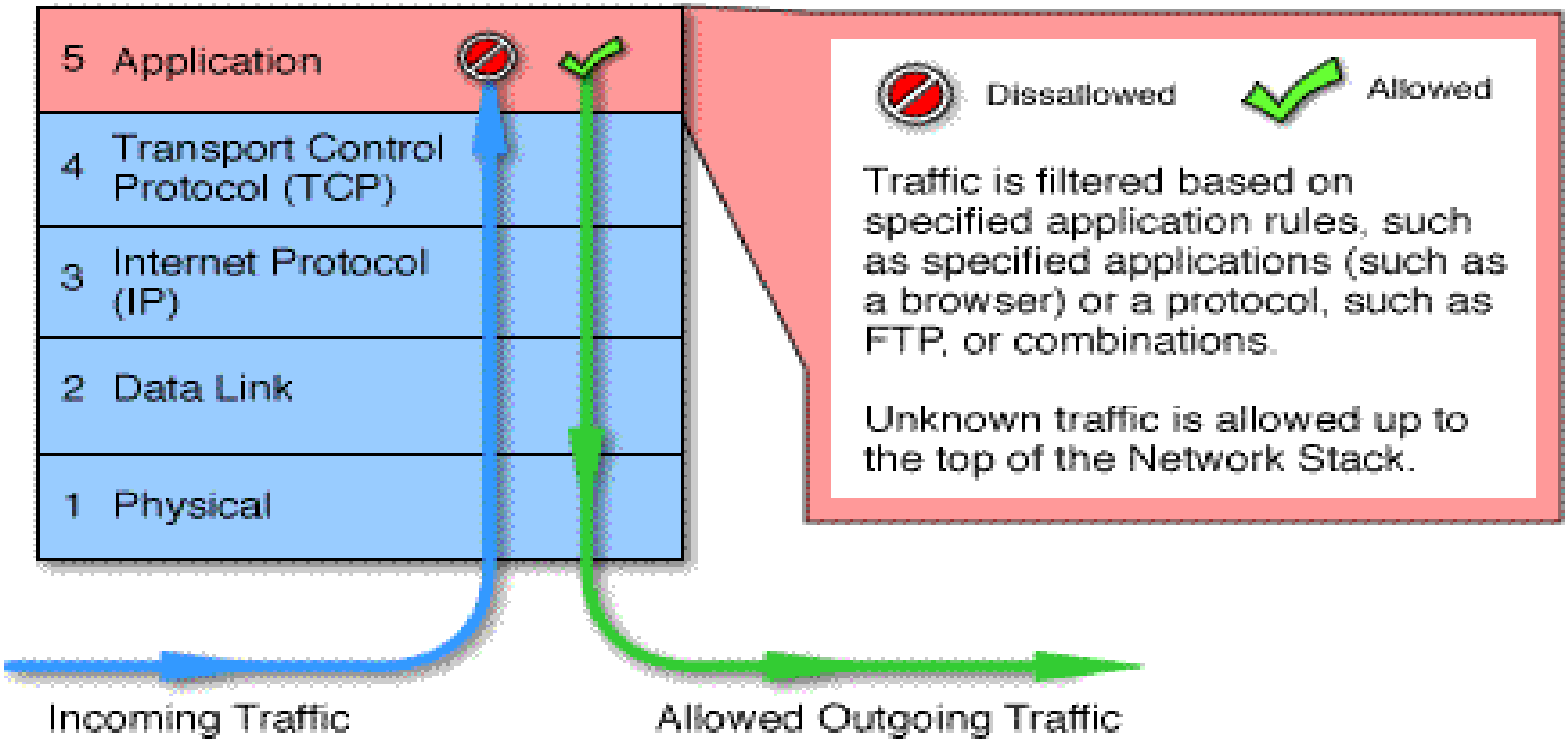
Paketifilter



http://www.crazylearner.org/wp-content/uploads/2013/05/packet-filter-firewall.png

Tulemüürid

Rakendusepõhine tulemüür



http://www.di.unisa.it/~ads/corso-security/www/CORSO-0102/astaro/app_layer_f.gif

Tulemüür OSI mudelis

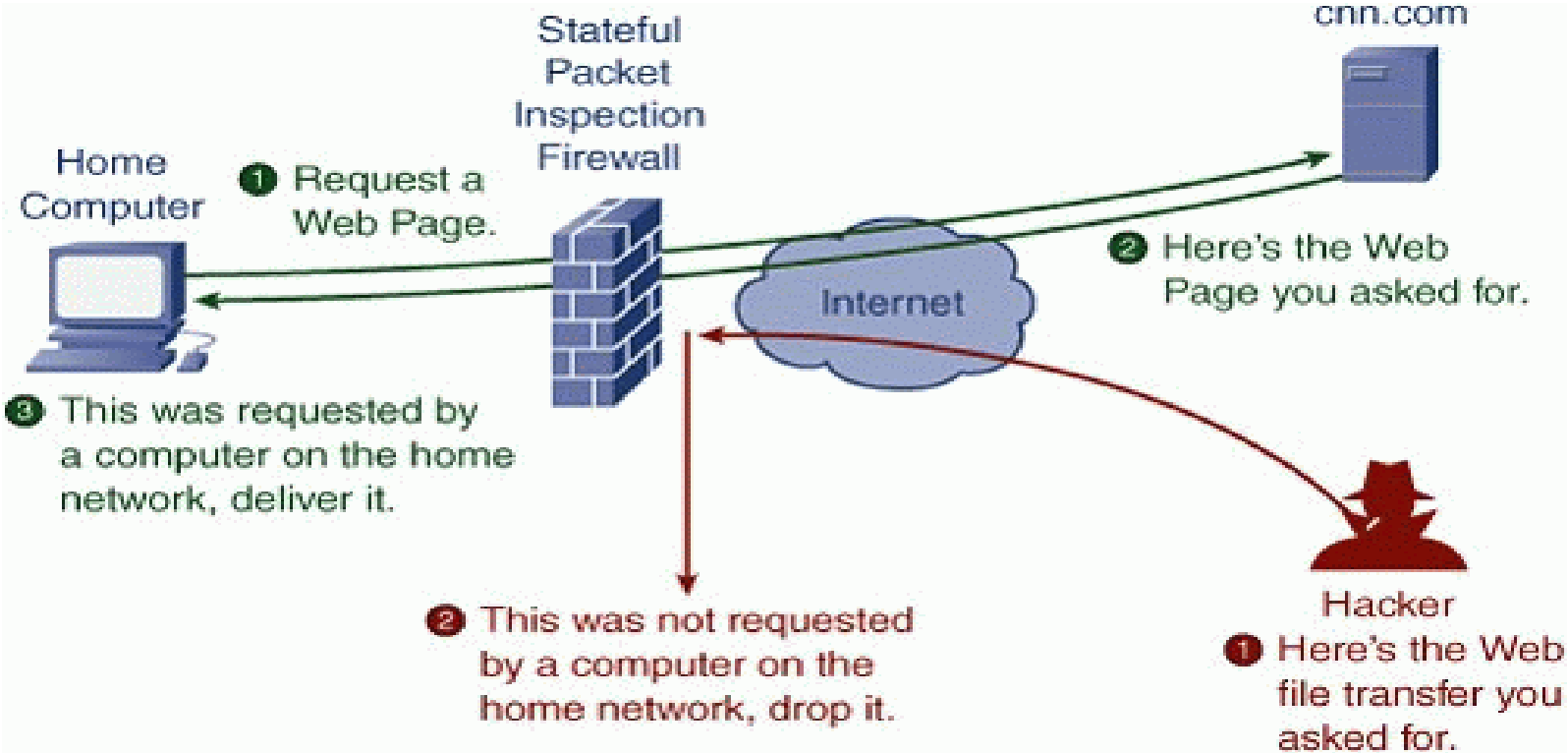
OSI - *Open Systems Interconnection*

OSI mudel	PDU Protocol Data Unit		
7. Rakenduskiht *Application layer*	*Data*	Rakenduspõhine tulemüür *application-layer firewall (3rd generation firewall)*	Teevad otsuseid IP-paketi sisu alusel (nt konkreetsed veebilehed, pahavara jms)
6. Esitluskiht *Presentation layer*			
5. Seansikiht *Session layer*		Aheltulemüür *circuit gateway / firewall* TCP/UDP ühenduste turvalisus, jälgitakse TCP paketi kätlust *(handshaking)*, tulemüüri reeglite ja poliitikate täitmist *(2nd gen FW)*	Kui veebipäring läheb läbi aheltulemüüri, kasutajapõhine info filtreeritakse (nt IP-aadress). Puhverserver edastab päringu veebiserverile. Vastust saates väline server näeb puhverserveri IP-aadressi kuid mitte midagi võrgusisese kasutaja (päringu tegeliku saatja) kohta. Veebi- vms välisvõrgus asuv server vastab puhverserverile, mis edastatakse aheltulemüüri poolt kliendile.
4. Transpordikiht *Transport layer*	*Segment (TCP) / Datagram (UDP)*		
3. Võrgukiht *Network layer*	*Packet*	Paketifilter *packet filter (1st gen FW)*	IP-pakettide filtreerimine, otsused tehakse IP paketi päiseinfo alusel (näiteks lähte/siht aadressi/pordi alusel)
2. Andmevahetuskiht *Data link layer*	*Frame*	Andmevahetuskihi tulemüür *MAC-layer firewall*	*Andmevahetuskihi MAC alamkihil toimub pakettide filtreerimine vastavalt ligipääsunimekirjas (ACL) olevatele kirjetele, mis seotud konkreetsete MAC-aadressidega.*
1. Füüsiline kiht *Physical layer*	*Bit*		

Tulemüüri vajadus

- Mille jaoks on vaja?
  - Lubades ühendused vaid teatud teenustele ja teatud arvutitest
  - Lubades väljuvaid ühendusi vaid lubatud arvutitest ja lubatud teenuste külge
  - Edastada pakette vastavalt etteantud reeglitele (näiteks ühenduse jagamine)
  - Piirata/häälestada liiklust - erinevate teenuste paketid saavad erinevalt käsitletud. Näiteks saab seada piirangu andmemahule – mida ISP'd teevad.
  - Sisevõrgu teenused ei pruugi kõik Internetis nähtavad olla (nt vaid VPN'i vahendusel)

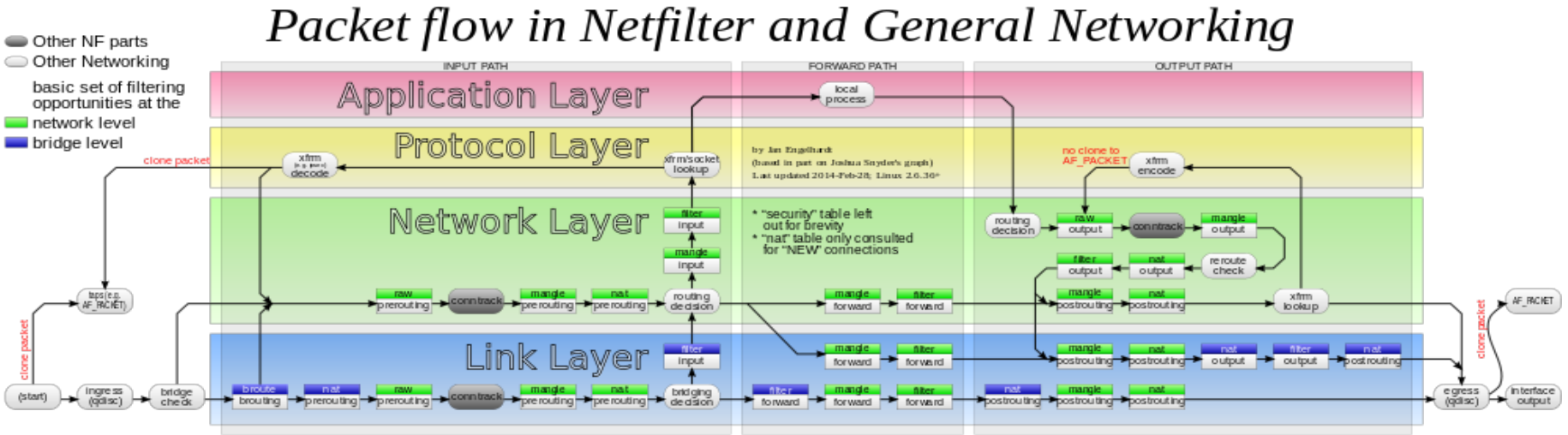
Tulemüüri ülevaade



http://2.bp.blogspot.com/-Iblk0555nyY/UB-NbNjYpHI/AAAAAAAAAMw/fr6KGlr63JE/s1600/8-6+firewall1.gif

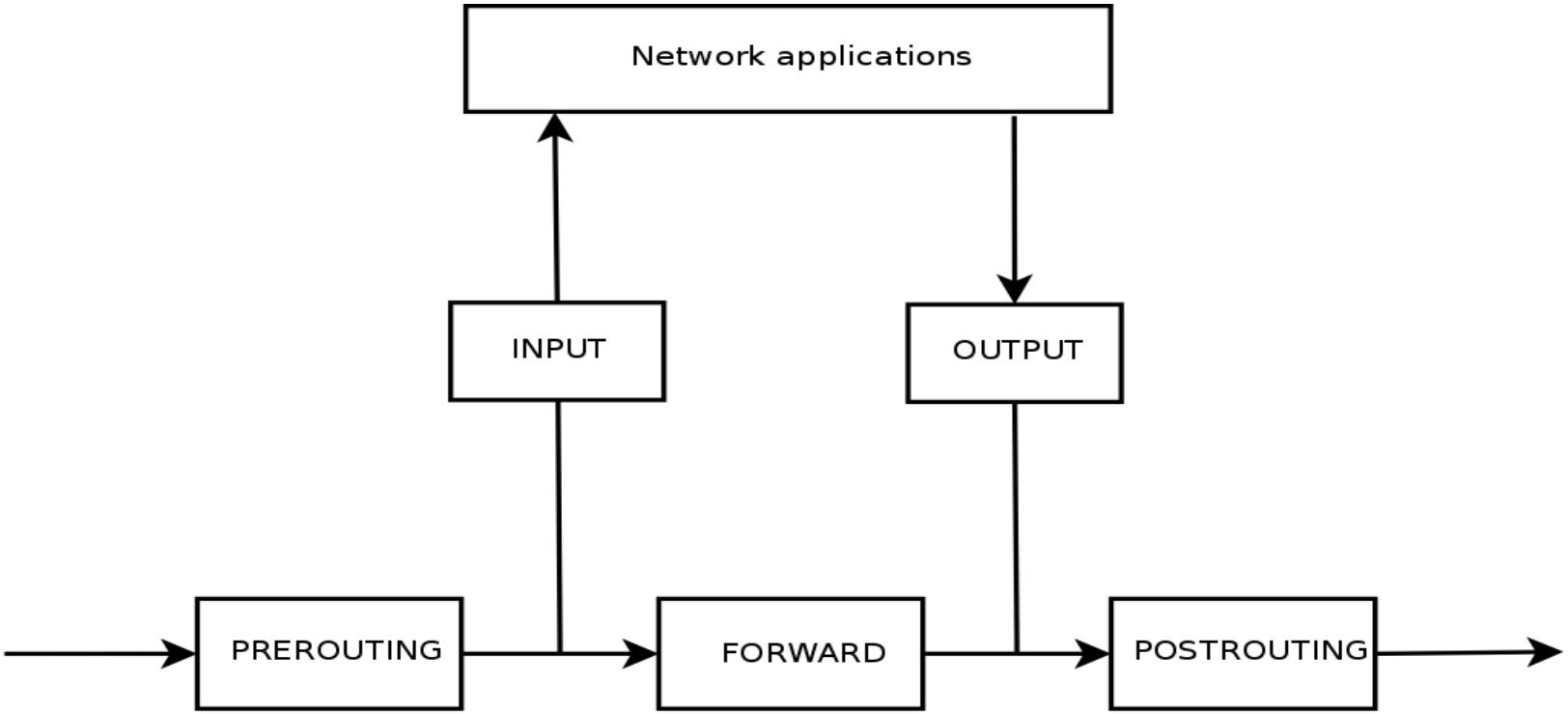
Netfilter Linuxis

Programm *iptables* on mõeldud Linux võrgupakettide filtreerimistarkvara *netfilter* seadistamiseks



https://en.wikipedia.org/wiki/Firewall_(computing)#/media/File:Netfilter-packet-flow.svg

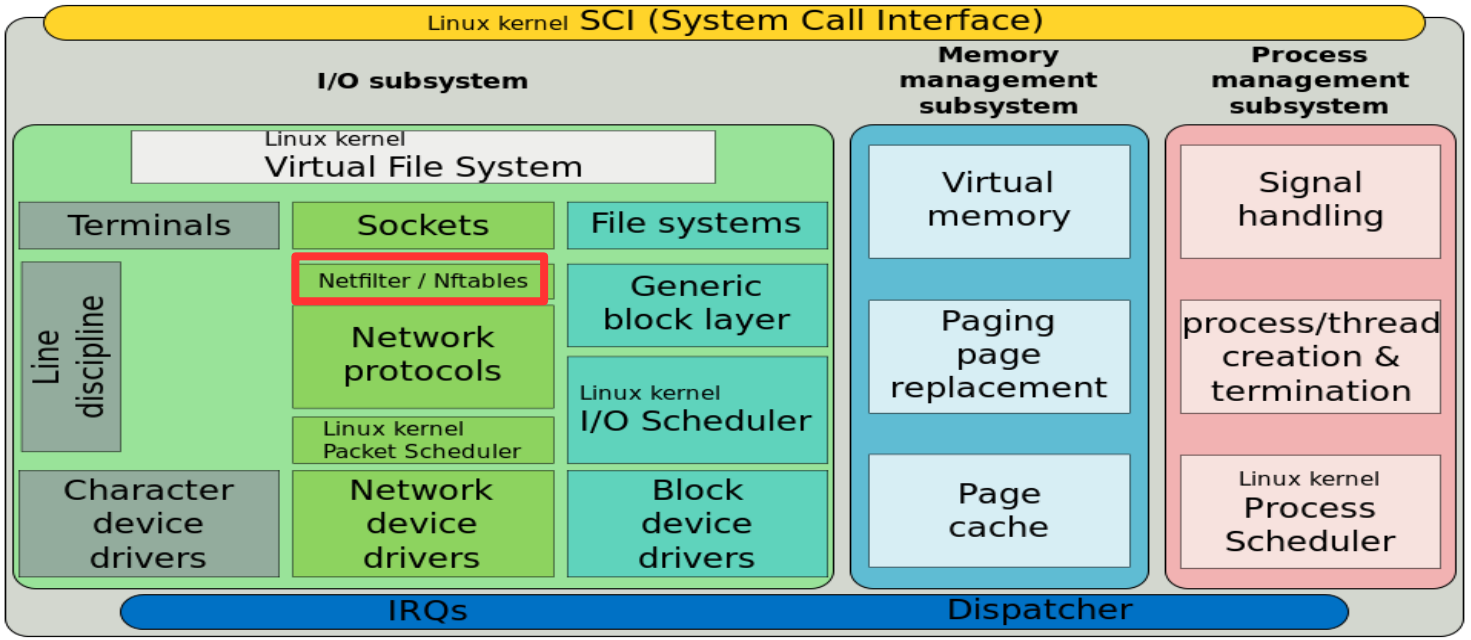
Netfilter



https://debian-handbook.info/browse/stable/images/netfilter.png

nftables Linuxis

- alates 3.13 tuuma versioonist
  - https://launchpad.net/ubuntu/+source/nftables
  - https://home.regit.org/netfilter-en/nftables-quick-howto/
  - http://askubuntu.com/questions/517136/list-of-ubuntu-versions-with-corresponding-linux-kernel-version
  - https://en.wikipedia.org/wiki/List_of_Ubuntu_releases#Table_of_versions
- mõeldud asendama *netfilter*'it



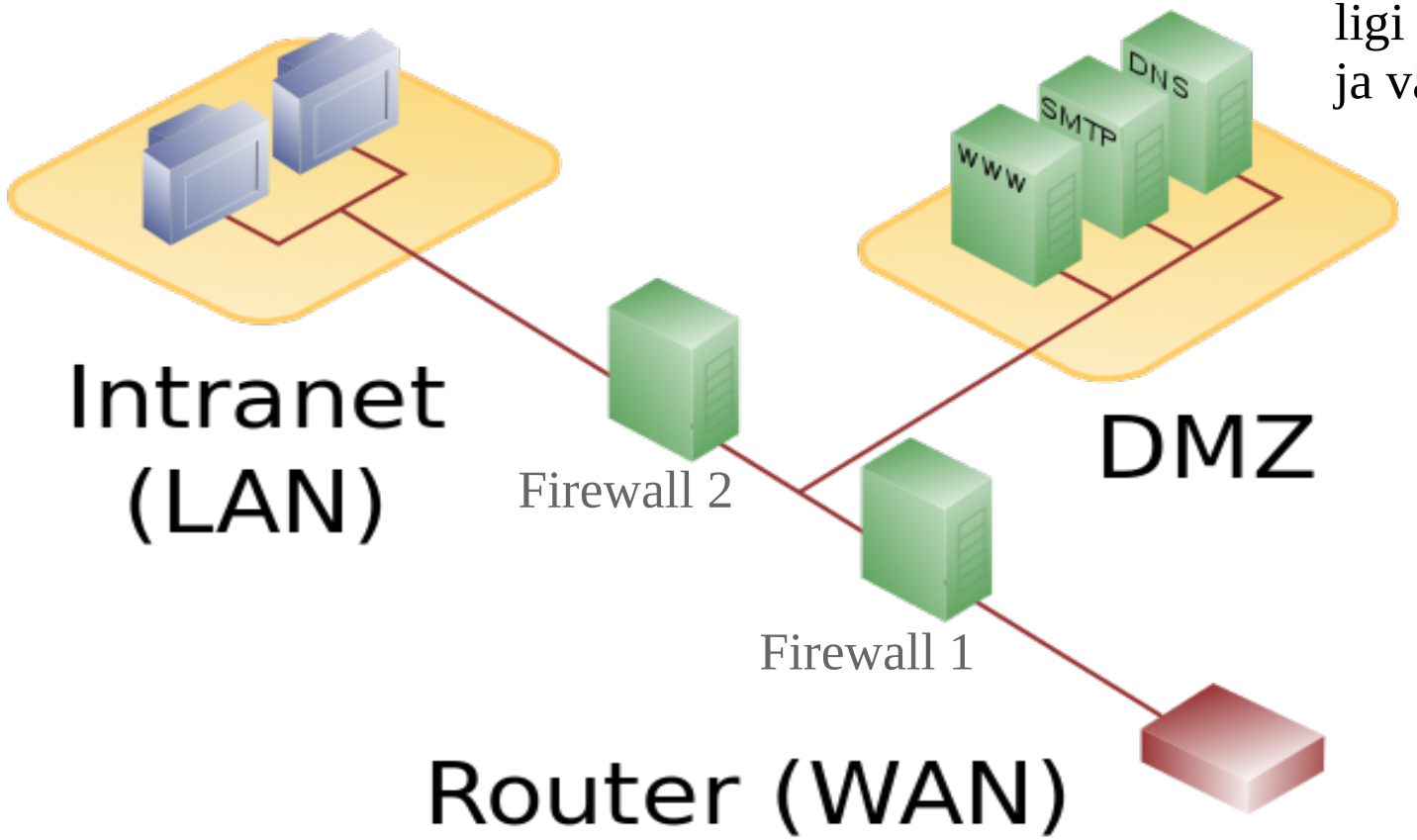
https://en.wikipedia.org/wiki/Nftables
https://en.wikipedia.org/wiki/Nftables#/media/File:Simplified_Structure_of_the_Linux_Kernel.svg

DMZ 1

- DMZ - *demilitarized zone*
- Eraldamaks välisvõrgule pakutavaid teenuseid sisevõrgust
- Sise- ja välisvõrgust saab kasutada DMZ tsoonis asuvaid teenuseid
- Eraldajateks on tulemüürid
- DMZ – kõige ohtlikum tsoon, kus madin käib :)

DMZ 2

Teenustele saab ligi võrgu seest ja väljast

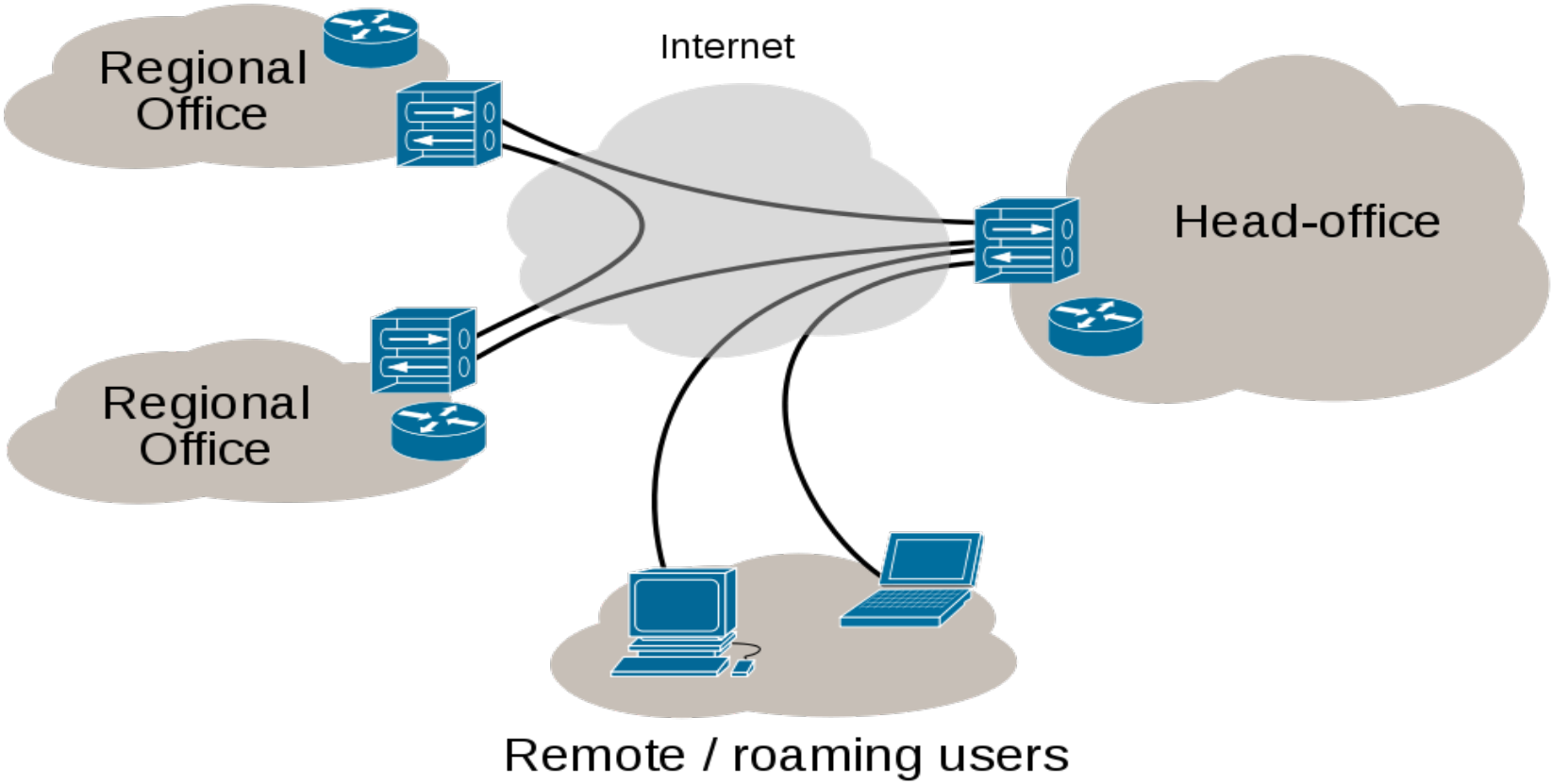


http://upload.wikimedia.org/wikipedia/commons/thumb/6/60/DMZ_network_diagram_2_firewall.svg/640px-DMZ_network_diagram_2_firewall.svg.png

VPN

- VPN - *Virtual Private Network*
- Laialdaselt kasutusel sisevõrgu teenuste poole pöördumiseks (nt ligipääs tasulistele andmebaasidele raamatukogus)
- Kasutaja tuvastatakse ja võrguliiklus krüpteeritakse
  - Anonüümne ründaja sisevõrguteenustele ligi ei pääse
  - Arvutis olev viirus siiski pääseb :(
- Mõnel firmal pole sisevõrku ja kõik teenused on kasutatavad läbi VPN ühenduste
- sshuttle – kiire lahendus OpenSSH serveri abil VPNi loomiseks (GNU/Linux, macOS, FreeBSD, OpenBSD, pfSense; testimist vajab MS Windows + WSL2). Piisab tarkvara paigaldamisest ja on ühendumiseks valmis!

VPN’i ülevaade

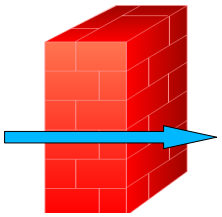


https://en.wikipedia.org/wiki/Virtual_private_network#/media/File:Virtual_Private_Network_overview.svg

Võrguaadresside teisendamine 1

- **NAT** (*Network Address Translation*) – võrguaadresside teisendamine (erinevate aadressruumide ühendamine võrguaadressi muutmisega IP paketi päises)
  - https://en.wikipedia.org/wiki/Network_address_translation
  - http://www.ipv6.com/articles/nat/NAT-In-Depth.htm
- **DNAT** (*Destination NAT*) välisvõrguaadressi muutmine sisevõrguaadressiks; kasutusel: *port forwarding, DMZ* – päringud välisvõrgust sisevõrku

SourceIP: 193.40.xxx.xxx
Dest IP: 193.40.194.200



SourceIP: 193.40.xxx.xxx
Dest IP: 172.16.0.170

Tulemüür teisendab saaja aadressi (*Dest IP*)

Sisevõrk

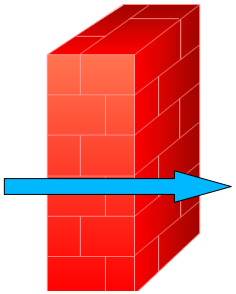
Sisevõrgu IP-aadressid

- IPv4 aadressid (RFC 1918)
  - 10.0.0.0 – 10.255.255.255, arv: 16 777 216 (24 bit = 2^{24})
  - 172.16.0.0 – 172.31.255.255, arv: 1 048 576 (20 bit = 2^{20})
  - 192.168.0.0 – 192.168.255.255, arv: 65 536 (16 bit = 2^{16})
- IPv6 aadressid (RFC 4193)
  - fc00::/7, arv: 2^{121}
- seade ise (*localhost*):
  - IPv4 127.0.0.1
  - IPv6 ::1
- vt ka reserveeritud IP-aadressid
  https://en.wikipedia.org/wiki/Reserved_IP_addresses

Võrguaadresside teisendamine 2

- **SNAT** (Source NAT) – sisevõrguaadressi teisendamine välisvõrguaadressiks, kasutus: päringud sisevõrgust välisvõrku (levinumaid)

SourceIP: 192.168.10.15
Dest IP: 193.40.194.200



SourceIP: 193.40.194.2
Dest IP: 193.40.194.200

Sisevõrk

Tulemüür (193.40.194.2) teisendab lähteaadressi (saatja) (Source *IP*)

ufw

- Tulemüürides ja ka muudes arvutisüsteemides on vajadus filtreerida IP pakette
- Ubuntu kasutab vaikimisi:
  ufw (*uncomplicated firewall*) (CLI)
  gufw (GUI) – võimalik ka üle võrgu teise masina tulemüüri seadistada (sh MS Windows'ist) – peab olema *gufw* versioon 13.10.2 või uuem
- on CLI kasutajaliides *iptables*'ile kuid ei võimalda kõike ent samas on lihtsam kasutada
- https://help.ubuntu.com/community/UFW
- https://help.ubuntu.com/lts/serverguide/firewall.html

ufw 2

- **ufw [--dry-run] [options] [rule syntax]**
  - *--dry-run* simuleerib kuid ei rakenda
  - kasutatakse lihtsat süntaksit (pordi number ja soovi korral ka protokoll)
  - reeglid asuvad */etc/ufw/*.rules*
  - logifail */var/log/ufw.log*
  - seaded */etc/default/ufw* ja */etc/ufw/*.conf*
  - reeglite järjekord on oluline
    - esimesed loetakse kõigepealt sisse
    - detailsemad enne
    - üldisemad pärast
  - rakenduste profiilid (.ini süntaksiga)
    - */etc/ufw/applications.d/ ja* vaadatakse ka faili */etc/services*
    - GUI */etc/gufw/app_profiles/*
  - *man ufw (man gufw)*

ufw options (valik)

- *allow* – lubamine (edasi ei uurita)
- *deny* - lükkame tagasi ja ei anna sellest teada
- *reject* – lükkame tagasi ja anname sellest teada
- *limit* – *DoS, DDoS* tõrjumiseks
  (veendu, et IPv6 toetatud – *man ufw*)
  (vaikimisi peale 6.katset blokeeritakse 30 sekundiks)
- *status* – kas ufw on sisse lülitatud või mitte
- *show* – hetkel kehtivad reeglid
- *reset* – keelab ja taastab algseaded
- *reload* – laadib reeglid uuesti

ufw baassüntaks

- Lülita sisse/välja (sh ka peale arvuti taaskäivitamist):
  - *ufw [--dry-run] enable*|*disable*|*reload*
- Portide lubamine/keelamine:
  - *sudo ufw allow*|*deny*|*reject port*|*[/protocol]*
  - *protocol: tcp, udp*
    - *sudo ufw allow 22*
    - sudo ufw allow 22/tcp
  - vaikimisi keelatakse sisenev (in) kuid võib ka väljuva keelata,
    nt *sudo ufw reject out ssh*

ufw baassüntaks 2

- Reegli kustutamine
  - reegel: *sudo ufw deny 80/tcp*
  - kustutamine: *sudo ufw **delete** deny 80/tcp*
- Teenuste nimed ja pordid
  - *less /etc/services* (väljumiseks q)
  - *sudo ufw allow|deny servicename*
    - *sudo ufw allow ssh* (lülitatakse nii tcp kui udp)
    - *sudo ufw allow ssh/tcp* (ainult tcp)
  - teenusenime kasutamisel vaadatakse faili */etc/services* ja kui seal vastav nimi olemas siis lülitatakse sisse kõik sellega seotud pordid

ufw baassüntaks 3

- logimine
  - *sudo ufw logging <on/off/LEVEL>*
  - *LEVEL: off, low, medium, high, full; on=low*
    - *sudo ufw logging on*
- seisundi uurimine
  - *sudo ufw status*
  - *sudo ufw status [verbose, numbered]*
  - *sudo ufw app list* (saadaolevad rakenduste profiilid)

ufw näidis

- vaatame hetke poliitikat
  - **grep 'DEFAULT_' /etc/default/ufw**
  - *DEFAULT_INPUT_POLICY="REJECT"*
  - *DEFAULT_OUTPUT_POLICY="ACCEPT"*
  - *DEFAULT_FORWARD_POLICY="DROP"*
  - *DEFAULT_APPLICATION_POLICY="SKIP"*
- enne tulemüüri sisselülitamist keelame kogu siseneva liikluse
  - *sudo ufw default deny* (vaikimisi rakendatakse sisenevale liiklusele)
  - täpsemalt saab:
    - *sudo ufw default allow outgoing*
    - *sudo ufw default deny incoming*
- lubame SSH serveriga ühendumiseks
  - *sudo ufw allow ssh*
- lülitame tulemüüri sisse
  - *sudo ufw enable*

ufw näidis 2

- kui SSH lubatud ja tulemüür töötab siis edasi saame juba eemalt SSH kaudu ligi
- saame hakata lisama teenuseid tulemüüri
- vaatame seisundit
  - *sudo ufw app list* (saadaolevad rakenduste profiilid)
  - *sudo ufw status* (pordid, protokollid)
- lubame veebiserveri (lubatakse nii *tcp* kui *udp*)
  - *sudo ufw allow http* (või ka *sudo ufw allow 80/tcp*)
  - *sudo ufw allow https* (või ka *sudo ufw allow 443/tcp*)

ufw näidis 3

- lubame Samba (MS Windowsi failiserver)
  - *sudo ufw allow 137,138/udp*
  - *sudo ufw allow 139,445/tcp*
- kui vastava rakenduse profiil on olemas siis
  - *sudo ufw allow Samba*
  - profiili saab kopeerida */etc/gufw/app_profiles/samba.jhansonxi* asukohta */etc/ufw/applications.d/samba* (faililaiend ei ole oluline)
  - ligipääsu piiramine ühe alamvõrguga: *sudo ufw allow from 192.168.0.0/16 to any app Samba*
- lubame logimise (vaikimisi *low*): *sudo ufw logging on*

ufw rakenduse profiili näidis

- Samba profiili /etc/ufw/applications.d/samba näidis (nurksulgudes märksõna kasutatakse ufw reegli kirjutamisel):

[Samba]

title=SAMBA

description=SMB/CIFS protocol for Unix systems, allowing you to serve files and printers to Windows, NT, OS/2 and DOS clients

ports=137,138/udp|139,445/tcp

categories=Network;Services;|Network;File Transfer

reference=[http://www.samba.org/samba/docs/server_security.html]

- info mooduli kohta, nt CUPS:
  sudo ufw app info CUPS

ufw rakenduse profiil

- ühte faili */etc/ufw/applications.d/appsprofiles* võib ka mitme rakenduse profiilid kirjutada (profiilide failinime võib vabalt valida):

[puppet]

title=puppet configuration manager

description=Puppet Open Source from http://www.puppetlabs.com/

ports=80,443,8140/tcp

[AMANDA]

title=AMANDA Backup

description=AMANDA the Advanced Maryland Automatic Network Disk Archiver

ports=10080

ufw rakenduste profiilid

- sama rakenduse eri profiilid samas failis
  /etc/ufw/applications.d/appsprofiles

===start of apache2.2-common file===

[Apache]

title=Web Server

description=Apache v2 is the next generation of the omnipresent Apache web server.

ports=80/tcp

[Apache Secure]

title=Web Server (HTTPS)

description=Apache v2 is the next generation of the omnipresent Apache web server.

ports=443/tcp

[Apache Full]

title=Web Server (HTTP,HTTPS)

description=Apache v2 is the next generation of the omnipresent Apache web server.

ports=80,443/tcp

===end of file===

ufw näidis 4

- keelame ping’i
  - *failis /etc/ufw/before.rules*
    (IPv6 puhul before6.rules) muuta:
    # ok icmp codes
  - *-A ufw-before-input -p icmp --icmp-type destination-unreachable -j DROP*
  - *-A ufw-before-input -p icmp --icmp-type source-quench -j DROP*
  - *-A ufw-before-input -p icmp --icmp-type time-exceeded -j DROP*
  - *-A ufw-before-input -p icmp --icmp-type parameter-problem -j DROP*
  - *-A ufw-before-input -p icmp --icmp-type echo-request -j DROP*
- takistame rünnakud SSH pordile (⩾6 päringut 30 s jooksul)
  - *sudo ufw limit SSH (sudo ufw limit 22/tcp)*
  - *sudo ufw limit from 205.184.2.4 to tcp 22*

ufw musta nimekirja panemine

- failis /etc/ufw/before.rules

```
## blacklist section
# block just 199.115.117.99
-A ufw-before-input -s 199.115.117.99 -j DROP
# block 184.105.*.*
-A ufw-before-input -s 184.105.0.0/16 -j DROP
# don't delete the 'COMMIT' line or these rules won't be processed
COMMIT
```

ufw ruutimine (maskeraad)

- lubame pakettide edastamise */etc/default/ufw*
  - DEFAULT_FORWARD_POLICY="ACCEPT"
- lubame ka */etc/ufw/sysctl.conf* failis
  - net.ipv4.ip_forward=1
  - net.ipv6.conf.default.forwarding=1 #(kui kasutatakse ka IPv6'te)
- /etc/ufw/before.rules

 # nat Table rules

**nat*

:POSTROUTING ACCEPT [0:0]

 # Forward traffic from eth1 through eth0.

-A POSTROUTING -s 192.168.0.0/24 -o eth0 -j MASQUERADE

 # don't delete the 'COMMIT' line or these nat table rules won't be processed

COMMIT

- taaskäivitame ufw: *sudo ufw disable && sudo ufw enable*

ufw pordiedastus

- faili /etc/ufw/before.rules muuta:

```
# NAT table rules
*nat
:PREROUTING ACCEPT [0:0]
:POSTROUTING ACCEPT [0:0]
-F
# Port Forwardings
-A PREROUTING -i eth0 -p tcp --dport 22 -j DNAT --to-destination 192.168.1.10
# Forward traffic through eth0 - Change to match you out-interface
-A POSTROUTING -s 192.168.1.0/24 -o eth0 -j MASQUERADE
# don't delete the 'COMMIT' line or these nat table rules won't
# be processed
COMMIT
```

ufw ja moodulid

- failis */etc/default/ufw* on lõpus rida *IPT_MODULES="nf_conntrack_ftp nf_nat_ftp nf_conntrack_netbios_ns"*
- sellele eelnevad kirjeldused erinevatest moodulitest, mida saab lisada – kui moodul ei ole aktiivne siis tekivad probleemid vaatamata lubavatele reeglitele tulemüüris
- näiteks Samba puhul on oluline *nf_conntrack_netbios_ns*
- *uname -r* näitab, millise tuuma versiooni pealt töötatakse ja *dpkg --list* | *grep linux-image* näitab Ubuntu Linuxis paigaldatud tuumi
- seejärel saab kõiki ufw jaoks kasutatavaid mooduleid vaadata failist (x asemel konkreetne tuuma versioon) */usr/src/linux-headers-x.x.x-xxxxxx/net/netfilter/Kconfig*

ufw võimaldab ka täpsemalt

- keelame TCP-liikluse aadressilt 12.34.56.78 porti 22 kohalikus võrgus
  sudo ufw deny proto tcp from 12.34.56.78 to any port 22
- lubame ligipääsu IP-lt, võrgusegmendist
  - *sudo ufw allow from <ip address>*
  - *sudo ufw allow from 205.26.134.122*
  - *sudo ufw allow from 192.168.1.0/24*
- täpsustame ligipääsu lubamist:
  - *sudo ufw allow from <target> to <destination> port <port number>*
  - *sudo ufw allow from 192.168.0.4 to any port 22*

ufw täpsemalt...

- lubame täpsemalt
  - *sudo ufw allow from <target> to <destination> port <port number> proto <protocol name>*
  - *sudo ufw allow from 192.168.0.4 to any port 22 proto tcp*
- keelame täpsemalt
  - *sudo ufw deny from <ip address>*
  - *sudo ufw deny from 205.26.134.122*
- keelame koos pordinumbri ja protokolliga
  - *sudo ufw deny from <ip address> to <protocol> port <port number>*
  - *sudo ufw deny from 192.168.0.1 to any port 22*

ufw täpsem, näide

- keelame ligipääsu kahelt IP-aadressilt
  kuid teistele samas võrgusegmendis lubame porti 22
  - *sudo ufw deny from 192.168.0.1 to any port 22*
  - *sudo ufw deny from 192.168.0.7 to any port 22*
  - *sudo ufw allow from 192.168.0.0/24 to any port 22 proto tcp*
- siin pannakse täpsustavad reeglid enne kui üldine reegel – oluline on ka reeglite järjekord!

iptables

- *ufw* baasiks on *iptables*
- programm *iptables* on mõeldud Linuxi võrgupakettide filtreerimistarkvara *netfilter* seadistamiseks
- *netfilter/iptables* tarkvara võib jagada kaheks osaks
  - *tuuma* moodulid
  - *user space* tarkvara

Iptables võimalused

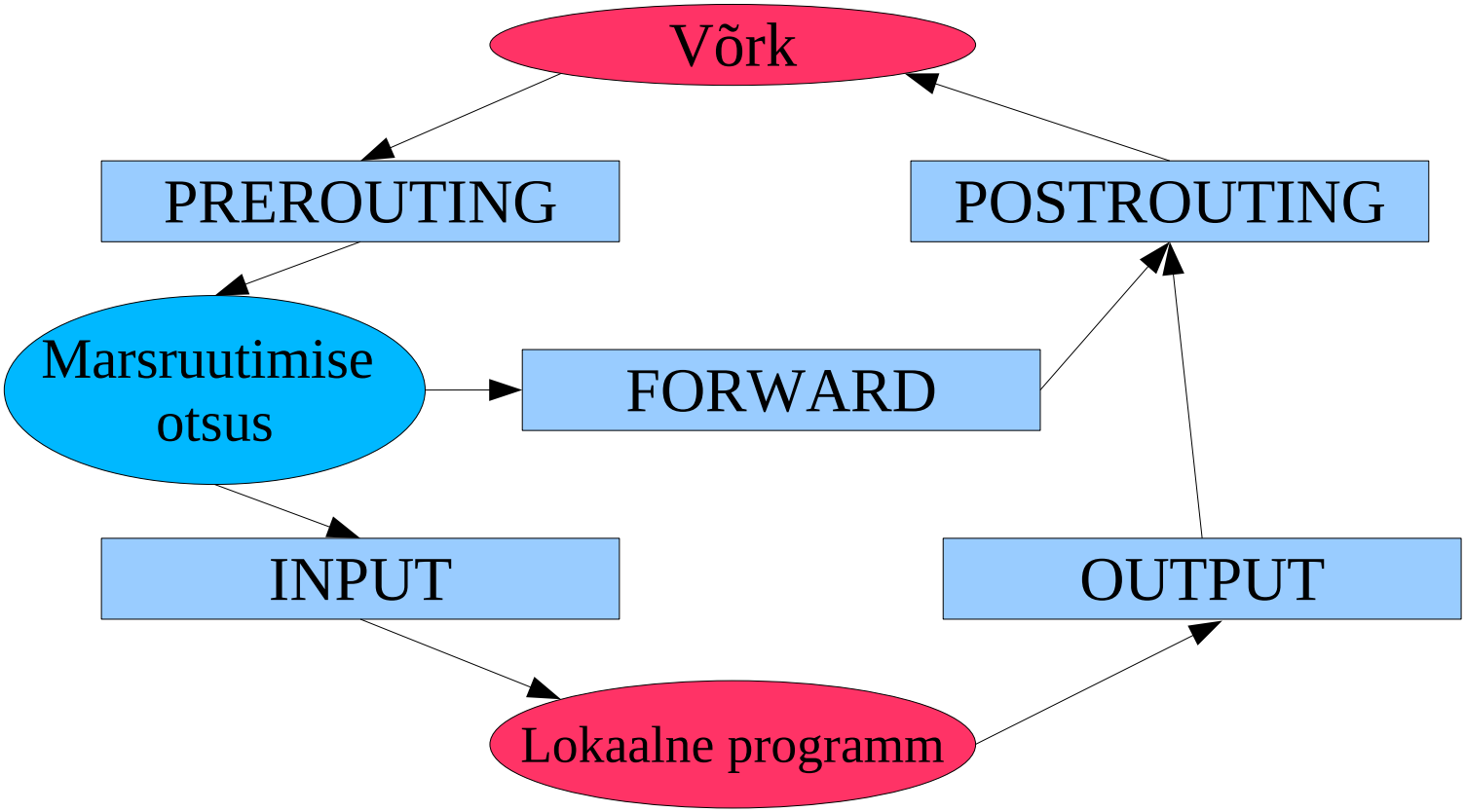
- Andmeside pakettide filtreerimine
- Ühenduste jälgimine (*connection tracking*)
- NAT (võrguaadresside teisendamine)
- *Mangling* (pakettide muutmine)
- Kiiruse piiramine
- Logimine

iptables tabelid ja ahelad

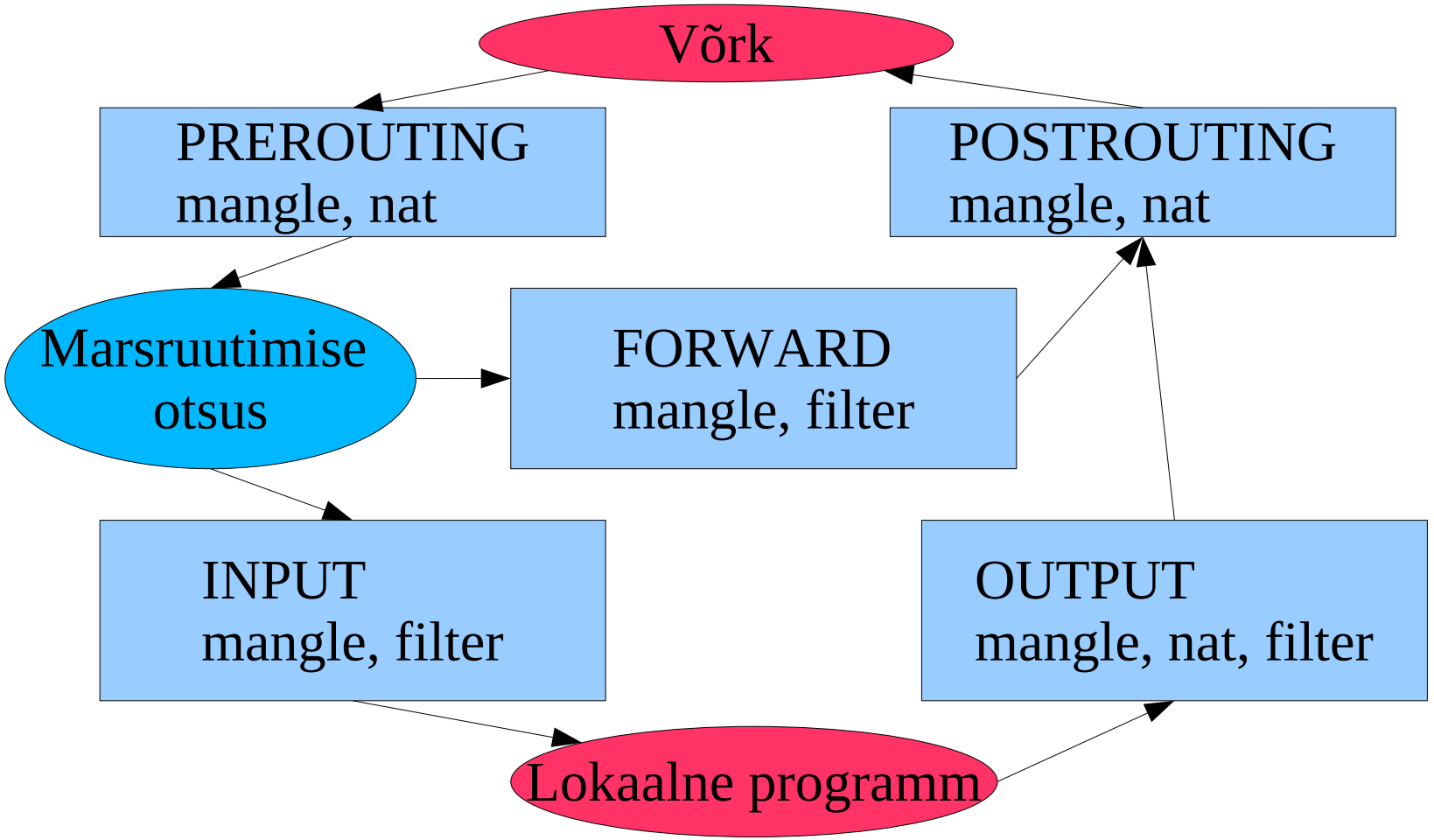
- Tabelid
  - Filter
  - Nat
  - Mangle
- Ahelad
  - Prerouting
  - Input
  - Output
  - Forward
  - Postrouting

- kõiki pakette pole vaja suunata läbi kõikide reeglite
- erinevad ahelad võimaldavad vähendada programmi poolt läbi uuritavaid tabeleid
- *man iptables*

iptables ahelad



iptables tabelid ja ahelad



http://www.iptables.info/en/structure-of-iptables.html

iptables tabelid

- Filter
  - Pakettide filtreerimiseks
    - FORWARD filtreerime edasi suunatavaid pakette
    - INPUT filtreerime sisenevaid pakette
    - OUTPUT filtreerime väljuvaid pakette
- Nat
  - Võrguaadresside transleerimiseks
    - PREROUTING aadressi transleerimiseks enne marsruutimist DNAT ehk destination NAT
    - POSTROUTING aadressi transleerimiseks peale marsruutimist SNAT source NAT
    - OUTPUT tulemüüri poolt teostatav NAT
- Mangle
  - Modifitseerime IP paketi päist
    - QoS bittide modifitseerimine

iptables käsu üldkuju

- **iptables [-t|--table table] -command [chain] [-i interface] [-p protocol] [-s address [port[:port]]] [-d address [port[:port]]] -j policy**
- Vaikimisi tabeliks on **filter**

iptables’i näited

- Keelame ära liikluse http pordi:
- *iptables -A INPUT -d 0.0.0.0/0 -p tcp --destination-port 80 -j REJECT*
  - REJECT – keeldume paketist ja anname sellest ka saatjale teada
- Lubame ühendused localhostist
  - *iptables -A INPUT -i lo -j ACCEPT*
- olemasolevate reeglite kuvamine
  - *iptables -L*

iptables näiteid

- suunamine
  iptables -t nat -A PREROUTING -p tcp --dport 80 -j REDIRECT --to-port 3127
  - Suunatakse porti 80 tulnud paketid porti 3127 (nt proxy)
- INPUT tabeli tühjendamine
  iptables -F INPUT

Maskeraadi näide

- *iptables --flush*
- *iptables --table nat --flush*
- *iptables --delete-chain*
- *iptables --table nat --delete-chain*
- *iptables --table nat --append POSTROUTING --out-interface eth1 -j MASQUERADE*
- *iptables --append FORWARD --in-interface eth0 -j ACCEPT*

iptables policy

- ACCEPT – lubamine. Edasi ei uurita
- DROP – blokeerimine. Edasi ei uurita
- LOG – logitakse sellele reeglile vastamine ja iptables jätkab reeglite uurimist
- REJECT – blokeerimine. Saatjale edastatakse vastus, et pakett blokeeriti (näiteks icmp-host-prohibited)
- DNAT – saaja aadress muutmine
- SNAT – saatja aadressi muutmine
- MASQUERADE – saatja aadress muudetakse tulemüüri omaks

iptables võtmed

- -t <-table> Tabel, vaikimisi filter
- -j <target> rakendatav policy
- -A lisab reegli
- -F Flush. Kustutab antud tabeli reeglid
- -p <protocol-type> Protokoll (icmp, tcp, udp ning all)
- -s <ip-address> Saatja IP
- -d <ip-address> Saaja IP
- -i <interface-name> Sisendseade
- -o <interface-name> Väljundseade
  - Näiteks ***iptables -A INPUT -s 0/0 -i eth0 -d 10.0.0.1 -p TCP -j ACCEPT***

iptables näide

- iptables -A FORWARD -s 0/0 -i eth0 -d 10.10.10.10 -o eth1 -p TCP --sport 1024:65535 --dport 80 -j ACCEPT
  - Lubame pakettide edastamise, kui pakett saadetakse IP aadressile 10.10.10.10, on pärit kaardist eth0 ja tuleb marsruutida eth1 kaudu. Ning lähteport peab jääma privilegeeritud portidest kõrgemale, ning sihtport peab olema http

iptables

- Soovitused
  - Tehke endale selgeks ahelad ja tabelid
  - Algajana kasutage konfigureerimise lihtsustamiseks iptables peale ehitatud tarkvara (otsingumootor on selle juures abiks)
  - Alustage lihtsamate reeglitega (filter)
  - Testige iga lisatud reegel ära
  - Salvestage reeglid faili ja kommenteerige need

iptables puudused

- Ei ole võimalust määrata mitut tegevust ühe reegli kohta a'la LOG + DROP, MARK + ACCEPT jne.
- Reeglite uuesti lugemine on vaevaline
- Sarnase koodi taaskasutus vähene (sama viga tuleb parandada mitmes kohas)
- Nftables – järgmine põlvkond (on mõeldud asendama ip, ip6, arp, ebtables ja ühel päeval ka iptables)

OpenBSD PF

- PF võrdlus iptables/netfilter vahenditega
  - Reeglid on loetavamad võrreldes iptables reeglitega.
  - Iptables võimaldab kasutada väliseid mooduleid
  - Erinevad jõudlustestid näitavad, et PF on parem stateful reeglitega tegelemisel (võtab reegli kohta vähem mälu)
  - OpenBSD SMP tugi pole samal tasemel Linux toega ja seega võib mitmetuumalistel tulemüüridel Linuxi jõudlus olla parem
  - OpenBSD eeliseks on süsteemi turvalisus

FirewallBuilder

- Paljud IT-süsteemide administraatorid eelistavad kommertstoodet, kuna soovivad saada kena konfigureerimisliidest.
- FirewallBuilder oskab genereerida reegleid mitmetele tulemüüridele
  - CISCO
  - BSD PF
  - Linux iptables
- https://wiki.itcollege.ee/index.php/FirewallBuilder
- http://www.fwbuilder.org/

Viiteid

- Ubuntus vaikimisi tulemüür ufw (GUI: gufw)
  https://wiki.itcollege.ee/index.php/Ufw
  https://wiki.itcollege.ee/index.php/Ubuntu_ruuter
  https://help.ubuntu.com/community/Firewall
  https://help.ubuntu.com/community/UFW
  https://wiki.ubuntu.com/UncomplicatedFirewall
  https://help.ubuntu.com/lts/serverguide/firewall.html
- https://wiki.itcollege.ee/index.php/Iptables
- Wikipedia - Comparison of firewalls
  http://en.wikipedia.org/wiki/Comparison_of_firewalls
- Netfilter ja iptables http://www.netfilter.org/
- Debian firewalls https://wiki.debian.org/Firewalls
- Uue põlvkonna tulemüürid https://en.wikipedia.org/wiki/Next-Generation_Firewall
- Design and Performance of the OpenBSD Stateful Packet Filter (pf)
  http://www.benzedrine.cx/pf-paper.html
- MS Windowsi tulemüür https://wiki.itcollege.ee/index.php/Windowsi_tulem%C3%BC%C3%BCr
- VPN https://wiki.itcollege.ee/index.php/Virtuaalsed_privaatv%C3%B5rgud

rünnakute tõrjumine:
• sshguard http://www.sshguard.net/
• fail2ban http://www.fail2ban.org/
alternatiivid:
• http://alternativeto.net/software/sshguard/
• http://alternativeto.net/software/fail2ban/

Küsimused?
Tänan tähelepanu eest!

IT KOLLEDŽ
TALLINNA TEHNIKAÜLIKOOL

TTÜ IT KOLLEDŽ

Raja 4C, 12616 Tallinn

tel +372 628 5800

info@itcollege.ee

http://www.itcollege.ee/