Tulemüürid

- Tulemüüri mõiste
- Tulemüüride liigitus
- Paketifiltrid
- Võrguaadresside tõlkimine (NAT)
- Rakenduskihi tulemüürid
- Kombineeritud tulemüürid
- Demilitariseeritud tsoon
- Üksiku arvuti kaitsmine
- Personaalsed tulemüürid
- Mida lubada ja mida keelata

Tulemüürid

- Tulemüür on seade, mis realiseerib sisevõrgu ja Interneti vahelist pääsupoliitikat
- Tulemüür kaitseb Internetist tulevate teatud liiki rünnete eest
  - Volitamata pöörduste eest
  - IP pinudes olevate vigade eest
  - (Mõnede) rakendustes olevate vigade eest
- Organiseerib liiklust kohtvõrgust Internetti
  - Võimaldab jagada teenused soovituteks ja soovimatuteks
  - Seda nii väljuval kui siseneval suunal

Tulemüüride liigitus

- Võrgukihi tasemel töötavad tulemüürid
  - Töötavad TCP/IP tasemel
  - (Staatilised) paketifiltrid
  - Dünaamilised paketifiltrid
- Rakenduskihi tasemel töötavad tulemüürid
  - Vahendajad (*proxy*'d)
- Kombineeritud tulemüürid

Lihtne tulemüür — paketifilter

- Lihtsaim lahendus tulemüüri realiseerimiseks
  - Realiseeritav enamuse ruuterite baasil
- Töötavad IP paketi tasemel: paketid lastakse läbi või "visatakse minema"
- Kriteeriumid filtreerimiseks:
  - Paketi lähte- ja sihtaadress
  - Protokoll
  - Kõrgema taseme protokolli (TCP, UDP) pordinumber
  - Lipud ja seansi algatamise tunnused
- Tehtav lisaks ka 2. kihis — tark sild ekraneerib (*screening*)

Paketifilter

- Paketifiltrite probleemid
  - UDP kui ühenduseta protokolli on raske filtreerida
  - TCP puhul on võimalikud poolavatud ühendused
  - Kas fragmendid läbivad alati filtri?
  - Mõned protokollid ei filtreeru
  - Hea paketifiltri kokkuseadmine on keeruline
- Dünaamilised paketifiltrid
  - Muudavad oma filtreid vastavalt läbivatele pakettidele
  - Ühenduste jälgimine (*connection tracking*)

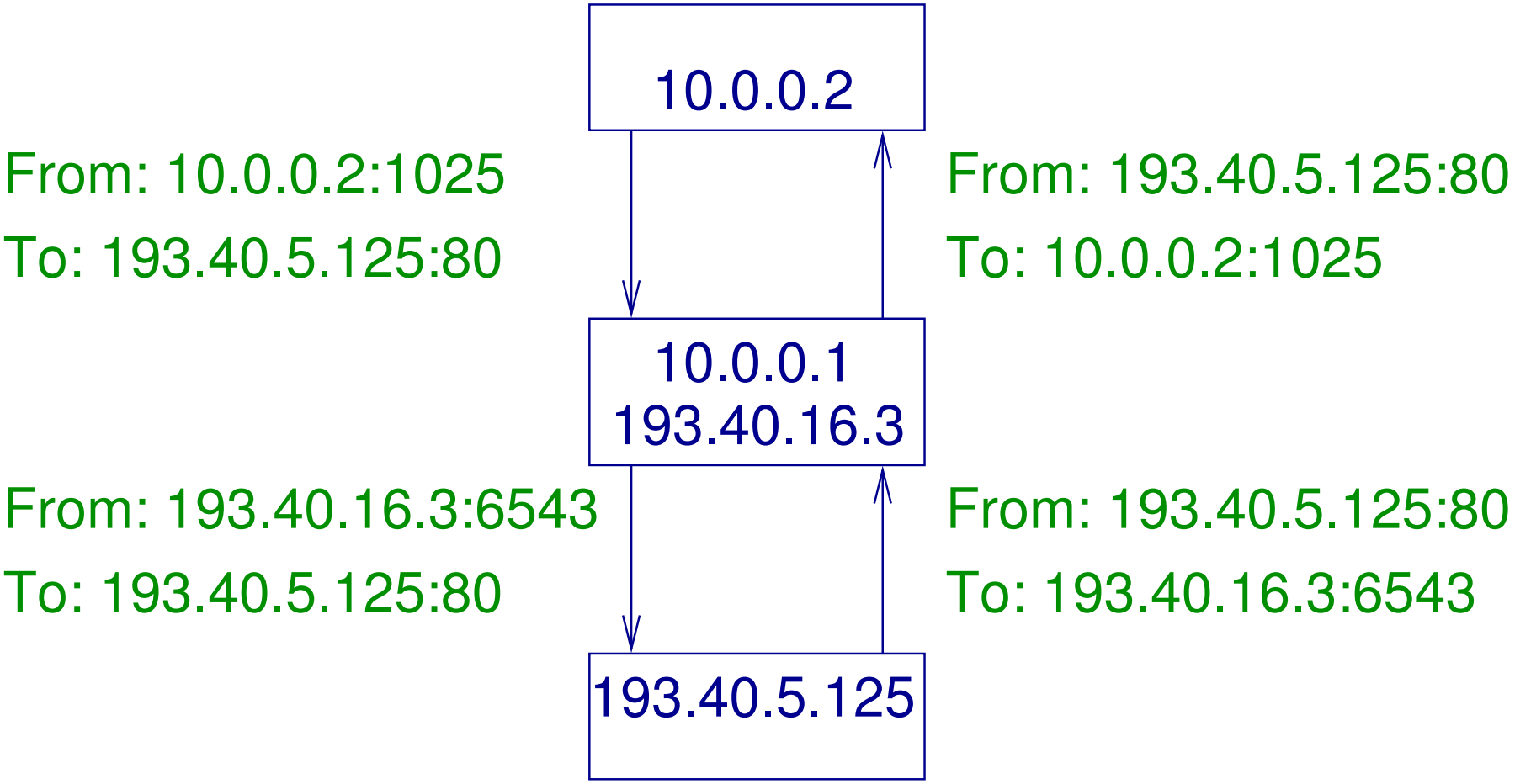
Võrguaadresside tõlkimine — NAT

- IPv4 aadressidega on kitsas käes, vaja on aadresside kasutamist optimeerida
- Tahame sisevõrgu struktuuri teiste eest ära peita
- Tahame, et sisevõrgu masinad ei oleks väljast otse nähtavad
- Lahendus(?): kasutame sisevõrgus privaataadresse, mis Internetis ei esine
- Vahel on siiski vaja pakette sise- ja välisvõrgu vahet liigutada
- Lahenduseks on aadresside tõlkimine ruuteris. Tõlkimist on kolme moodi:
  - Staatiline: $n - n$ — tõlgitakse terve aadressiplokk
  - Dünaamiline: $n - m$, $m < n$ — avalikke aadresse on vähem
  - Tõlkimine porte kasutades: $n - 1$ — kõik siseaadressid 1 välisaadressiks, varieeritakse lähtepordi numbrit

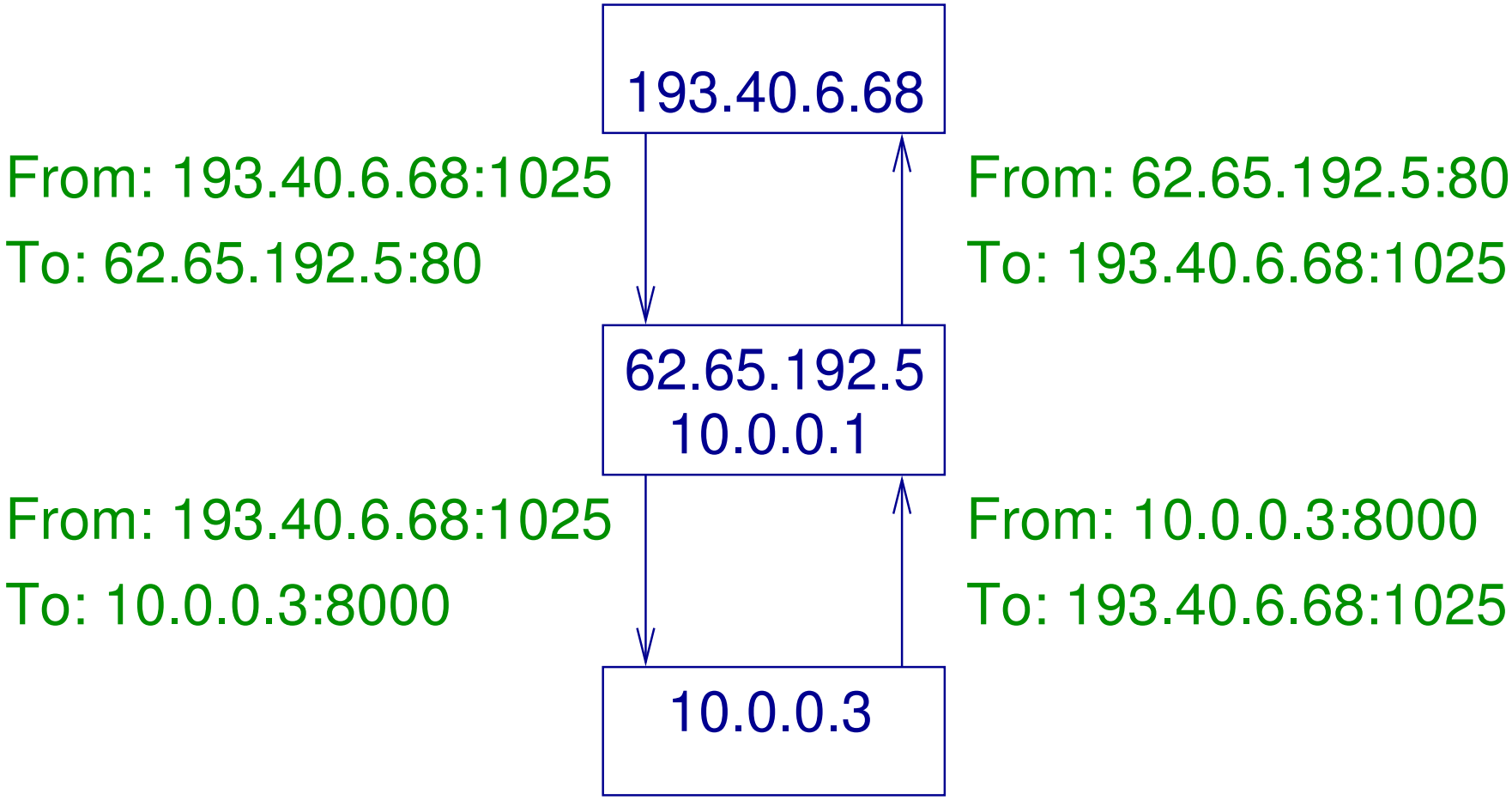
NAT tehnoloogia

- Standarditega on paika pandud aadressivahemikud, mida võib vabalt oma sisevõrkudes kasutada:
  - 10.*.*.*
  - 172.16.*.* – 172.31.*.*
  - 192.168.*.*
- Neid aadresse Internetis ei ruudita
- Aadresse tõlkiv ruuter modifitseerib ühe osapoole IP-aadressi (tõlgib ühe suuna andmed ning tõlgib tagasi vastused)
- Lähteaadressi maskeerimise abil saame varjata klientarvutit (algatajat) $\rightarrow$ SNAT
- Sihtaadressi maskeerimise abil saame varjata serverarvutit $\rightarrow$ DNAT

SNAT näide


10.0.0.2
From: 10.0.0.2:1025
To: 193.40.5.125:80
From: 193.40.5.125:80
To: 10.0.0.2:1025
10.0.0.1
193.40.16.3
From: 193.40.16.3:6543
To: 193.40.5.125:80
From: 193.40.5.125:80
To: 193.40.16.3:6543
193.40.5.125

DNAT näide


193.40.6.68
From: 193.40.6.68:1025
To: 62.65.192.5:80
From: 62.65.192.5:80
To: 193.40.6.68:1025
62.65.192.5
10.0.0.1
From: 193.40.6.68:1025
To: 10.0.0.3:8000
From: 10.0.0.3:8000
To: 193.40.6.68:1025
10.0.0.3

NAT probleemid

- Teeb katki TCP/IP mudeli, kus ainult ühenduse otspunktid teavad detaile
- Sunnib peale mingi osaliselt fikseeritud marsruudi otspunktide vahel
- Toob sisse ühe katkimineku punkti
- Toob sisse ühildumatuse paljude protokollidega
- Ei lahenda IPv4 aadresside kitsikust

AGA:

- Leevendab IPv4 aadresside kitsikust
- Aitab lihtsalt ja praktiliselt võrku turvalisemaks teha

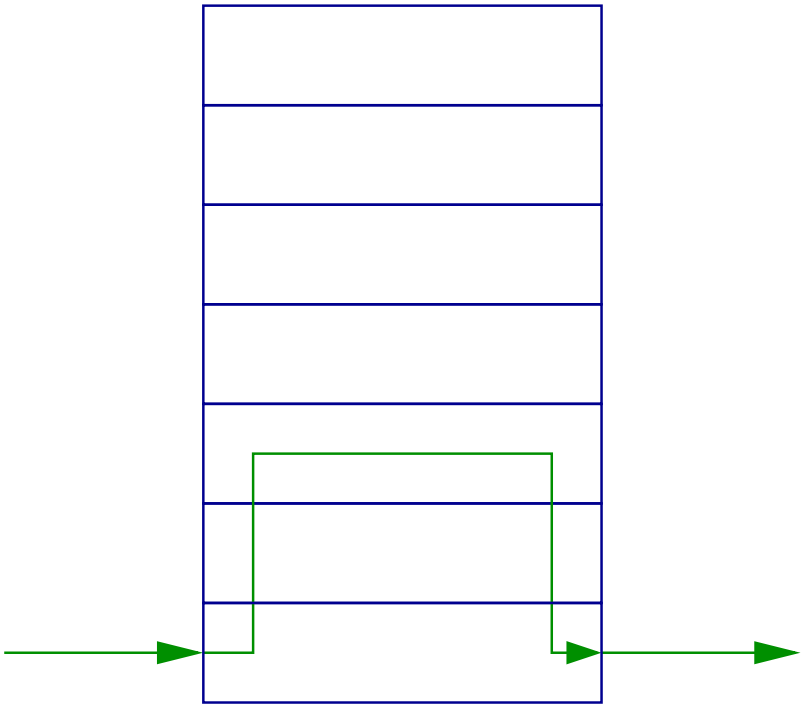
IPv6, tulemüürid ja NAT

- IPv6 reserveerib iga kohtvõrgu jaoks 2^{64} IPv6 aadressi
- Niimoodi on mugav teha automaatset IP-aadresside jagamist — iga arvuti saab genereerida oma IP-aadressi võrgu prefiksist ja oma MAC aadressist
- Kohtvõrgu arvutite skaneerimine on liiklusmahu tõttu võimatu
- Globaalne suur aadressivaru, NAT pole IPv6 jaoks kasutusel — lihtsalt lubame või keelame sisenevad ühendused, sisevõrgu struktuuri niikuinii teada ei saa eriti
- Uus probleem: privaatsus — sama MAC aadressiga arvuti on ära tuntav erinevate võrkude vahel liikudes, kuna IP-aadressi automaatselt genereeritud osa on sama
- Lahendus: IPv6 privaatsuslaiendused (juhuslik arv MAC aadressi asemel), oma piirangutega

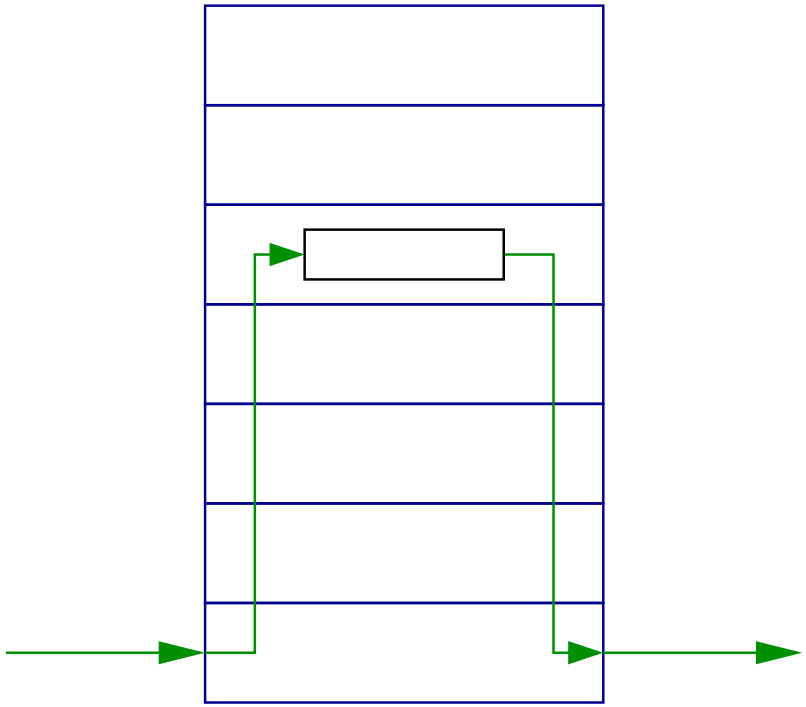
Rakenduskihi tulemüürid

- Kasutavad rakendusespetsiifiliste vahendajate tehnoloogiat
  - Läbipaistvad vahendajad (*transparent proxy*)
- Head küljed
  - Palju lisavõimalusi (antiviirused, WWW sisu analüüs, rämpsposti filtrid, . . .)
  - Hästi hallatavad ja konfigureeritavad
  - Puudub IP tasemel ühendus
  - Liikluse optimeerimine (nii valikuline lubamine kui puhverdamine)
- Vead
  - Iga protokoll vajab oma vahendajat
  - Rakendusprogrammid tuleb konfigureerida vahendajat kasutama

Tulemüürid eri kihtides



Võrgukihi tulemüür



Rakenduskihi tulemüür

Ühenduste sisu uurivad tulemüürid

- *Deep Packet Inspection*, *Next Generation Firewall*
- Käituvad paketifiltrina, aga vaatavad pakettide sisse kuni 7. kihini
- Panevad enda jaoks pakettidest kokku iga ühenduse andmevoo ja analüüsivad seda
- Dekodeerivad võimalusel ka rakenduskihi protokollid
  - Ei vaja selleks vahendaja konfimist või klientmasina teadmist vahendamise kohta
  - Võimalusel vaatavad ka krüpteeritud ühenduste sisse (oma CA vahendusrünnete tegemiseks, mida kliendid usaldavad)

Kombineeritud tulemüürid

- Lihtsate protokollide jaoks käituvad kui dünaamilised paketifiltrid (NAT)
- Keeruliste protokollide jaoks kasutatakse rakendustaseme vahendajaid
- Enamasti on võimalus mõningaid rakendustaseme vahendajaid kasutada läbipaistvana
- Enamus tänapäevaseid tulemüüre on kombineeritud tulemüürid

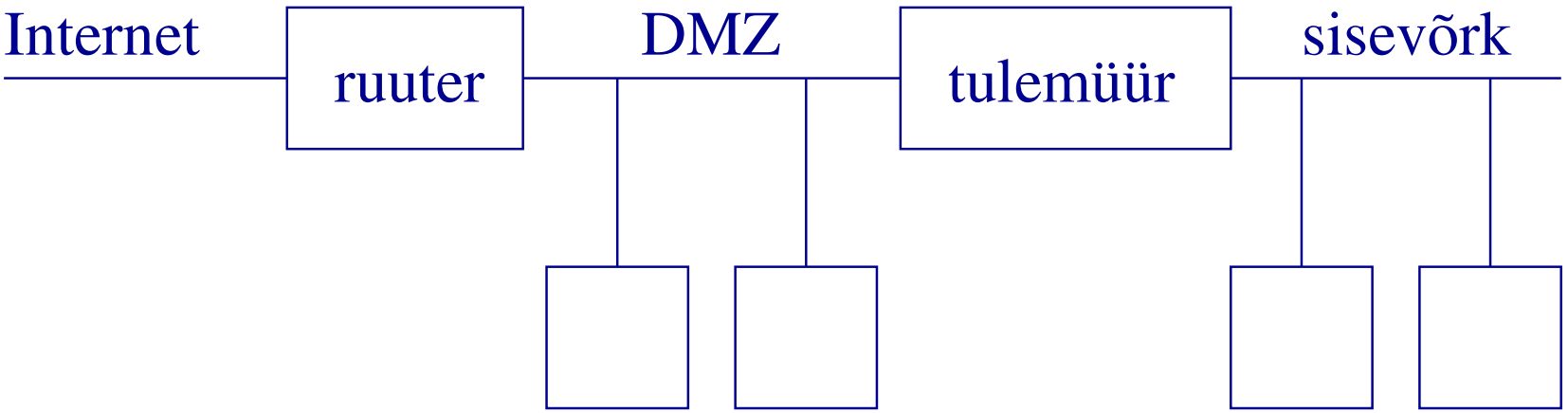
Mida väljastpoolt vaja on

- Vahel on siiski vaja väljastpoolt üht-teist kätte saada:
  - Meilide transport
  - Avalikud WWW, FTP serverid
  - Kaugtöötamine (näiteks juurdepääs kodust)
- Suuremate võrkude korral pannakse väljapoole tulemüüri eraldi serverid
- Väikese võrgu puhul pannakse teenused tihti tulemüüri peale
- Samuti on võimalik panna tulemüüri peale vahendaja, mis vahendab päringuid sisevõrgu serveri(te)le — rakendustaseme vahendaja või DNAT
- Enne väljast sisse suunduva lüüsi tegemist tuleb hoolikalt järele mõelda, kas seda on vaja ning kas sisevõrgus vastav programm on piisavalt turvaline

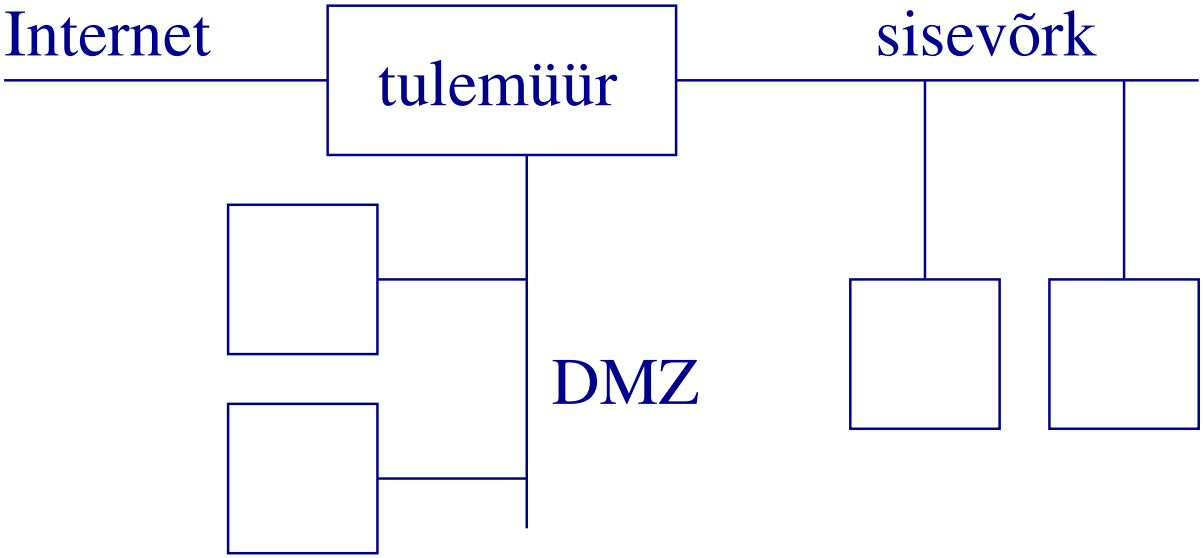
DMZ — demilitariseeritud tsoon

- Sisevõrgust eraldi asuv võrgupiirkond, mis on väljastpoolt kättesaadav
- Ei ole sisevõrk, ei ole ka väline Internet, on vahepealne ("demilitariseeritud")
- Avalike serverite hoidmiseks
- Sisevõrgust DMZ-i pääseb
- DMZ seest sisevõrku pääs puudub
- Kaks võimalust realiseerimiseks:
  - Tulemüüri ja välise filtreeriva ruuteri vahel
  - Eraldi segmendina tulemüüri küljes

DMZ tulemüüri ja välise ruuteri vahel



DMZ tulemüüri eraldi segmendina



Üksiku arvuti kaitsmine

- Juurdepääsufiltrid teenuses endas
- Veebiserveri domeenikaupa juurdepääsukontroll
- `tcp_wrappers`
- PAM moodulid
- Tänapäeval on lõppmasinas kasutatavad ka paketifiltrid

Personaalsed tulemüürid

- Traditsiooniline tulemüür on reeglina eraldi seade võrgu ees
- Personaalseteks tulemüürideks nimetatakse konkreetset personaalarvutit kaitsvat programmi
- Tavaliselt tegutsevad paketifiltrite tasemel
- Sisuline lisavõimalus: autentimine rakenduse kaupa
  - Kas rakendus tohib väljuvaid ühendusi luua?
  - Kas rakendus tohib väljast ühendusi vastu võtta?
- Vaikimisi on tihti mitmeid "auke" sees mugavuse säilitamiseks

Mida lubada ja mida keelata

- Väljuval suunal enamus asju lahti (välja pääseb)
  - Trooja hobused? Tunneldamine läbi HTTP?
- Väljava suuna ühenduste jälgimine (tagasi sisse lubatakse ainult vastusepakette)
- Sisse:
  - SMTP meilide jaoks (kui on oma meiliserver)
  - WWW, kui omal on server
  - Vajadusel ka sisenev login-teenus (ainult krüpteeritult — SSH, TLS baasil asjad, . . .)
  - Vajadusel ka postkastile juurdepääsu teenused (IMAP, POP3 — jällegi soovitavalt ainult krüptitud kujul)
  - Peer-to-peer võrgud???
  - Muud läheb väga harva vaja