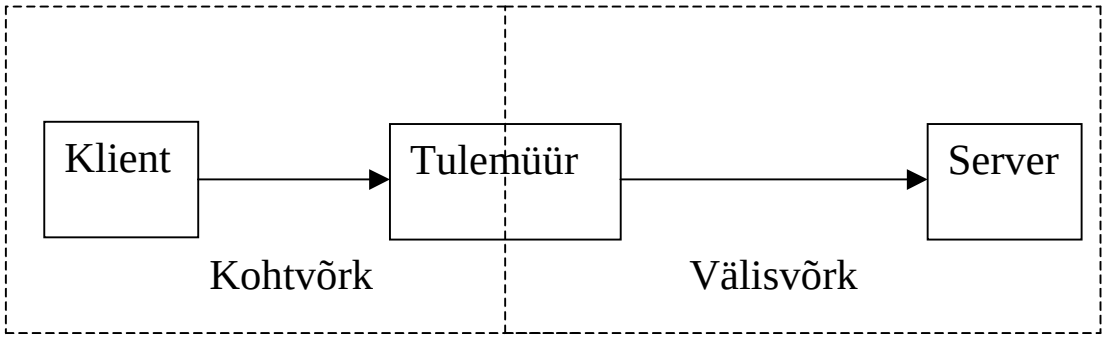
PAKETTIDE FILTREERIMINE TULEMÜÜRIDES

Filtreerimisreeglites kasutatavad TCP/IP pakettide parameetrid:

- Saatja IP aadress
- Vastuvõtja IP aadress
- IP teenust kasutav protokoll (TCP, UDP, ICMP)
- Saatja TCP/UDP port
- Vastuvõtja TCP/UDP port
- TCP *flag* ACK
- Paketi liikumise suund: “sisse” või ”välja”
- Teenuse pakkuja (serveri) asukoht: “sees” või “väljas”

NÄIDE 1 – Telnet “välja”



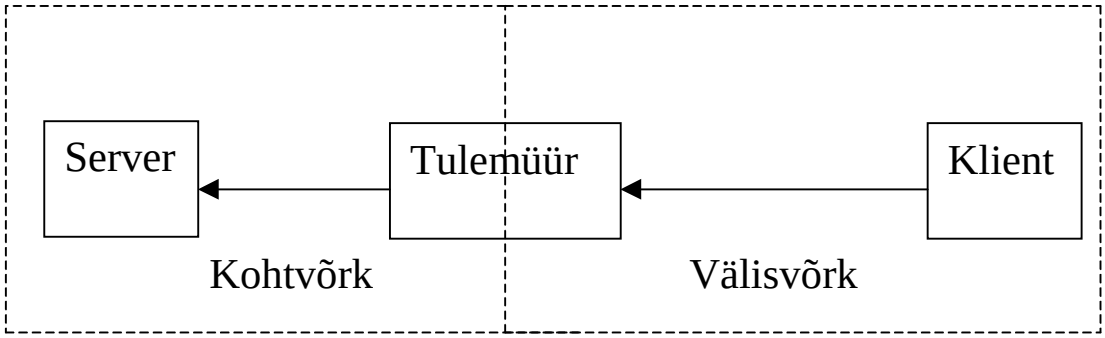
Kliendilt serverile (väljuv pakett):

- ✓ Saatja IP aadress = kohalik IP aadress (KA)
- ✓ Vastuvõtja IP aadress = suvaline välisvõrgu IP aadress (SA)
- ✓ Protokoll = TCP
- ✓ Saatja TCP port X = suvaline (>1023)
- ✓ Vastuvõtja TCP port = 23
- ✓ Kõige esimeses paketis kliendilt serverile ACK = 0, kõigis järgmistes ACK = 1

Serverilt kliendile (sisenev pakett):

- ✓ Saatja IP aadress = SA
- ✓ Vastuvõtja IP aadress = KA
- ✓ Protokoll = TCP
- ✓ Saatja TCP port = 23
- ✓ Vastuvõtja TCP port = X
- ✓ ACK = 1

NÄIDE 2 – Telnet "sisse"



Kliendilt serverile (sisenev pakett):

- ✓ Saatja IP aadress = välisvõrgu IP aadress (KA)
- ✓ Vastuvõtja IP aadress = kohtvõrgu Telnet-serveri IP aadress (SA)
- ✓ Protokoll = TCP
- ✓ Saatja TCP port Y = suvaline (>1023)
- ✓ Vastuvõtja TCP port = 23
- ✓ Kõige esimeses paketis kliendilt serverile ACK = 0, kõigis järgmistes ACK = 1

Serverilt kliendile (väljuv pakett):

- ✓ Saatja IP aadress = SA
- ✓ Vastuvõtja IP aadress = KA
- ✓ Protokoll = TCP
- ✓ Saatja TCP port = 23
- ✓ Vastuvõtja TCP port = Y
- ✓ ACK = 1

Kokkuvõte 1+2:

Serveri asukoht	Paketi suund	Saatja IP aadr	Vastuv. IP aadr	Prot	Saatja port	Vastuvõtja port	ACK
väljas	välja	kohal.	välis	TCP	X	23	0 / 1
väljas	sisse	välis	kohal.	TCP	23	X	1
sees	sisse	välis	kohal.	TCP	Y	23	0 / 1
sees	välja	kohal.	välis	TCP	23	Y	1

Filtreerimisreeglid juhul, kui lubatud on ainult väljuv Telnet ja ei midagi muud:

	Suund	Saatja aadr	Vastu võtja aadr	Proto	Saatja port	Vastuv õtja port	ACK	Otsus
A	välja	kohal	suva	TCP	>1023	23	0 / 1	OK
B	sisse	suva	kohal	TCP	23	>1023	1	OK
C	suva	suva	suva	suva	suva	suva	0 / 1	keela tud

Sobivat reeglit otsitakse järjekorras A -> B -> C

Näide 3.

1) Firmal on B-klassi alamvõrk 172.16.*.*
2) Ülikoolil on A-klassi alamvõrk 10.*.*.*
3) Firmal on koostööprojekt ülikooliga ja firma vastava projektosakonna alamvõrk on 172.16.6.*
4) Ülikoolis on “kahtlane” alamvõrk 10.1.99.* millest juurepääs mujale kui projektosakonna almvõrku peab olema välistatud

Firma tulemüüri filtreerimisreeglid:

Reegel	Saatja	Vastuvõtja	Otsus
A	10.*.*.*	176.16.6.*	OK
B	10.1.99.*	176.16.*.*	keelatud
C	suva	suva	keelatud

Katsetame (A -> B -> C):

Paketi jrk. Nr.	Saatja	Vastuvõtja	Soovitav otsus	Tegelik otsus (reegel)
1	10.1.99.1	172.16.1.1	keelatud	keelatud (B)
2	10.1.99.1	172.16.6.1	OK	OK (A)
3	10.1.1.1	172.16.6.1	OK	OK (A)
4	10.1.1.1	172.16.1.1	keelatud	keelatud (C)
5	192.168.3.4	172.16.1.1	keelatud	keelatud (C)
6	192.168.3.4	172.16.6.1	keelatud	keelatud (C)

Reeglite järjekord on tähtis:

Reegel	Saatja	Vastuvõtja	Otsus
B	10.1.99.*	176.16.*.*	keelatud
A	10.*.*.*	176.16.6.*	OK
C	suva	suva	keelatud

Katsetame (B -> A -> C):

Paketi jrk. Nr.	Saatja	Vastuvõtja	Soovitav otsus	Tegelik otsus (reegel)
1	10.1.99.1	172.16.1.1	keelatud	keelatud (B)
2	10.1.99.1	172.16.6.1	OK	keelatud (B)
3	10.1.1.1	172.16.6.1	OK	OK (A)
4	10.1.1.1	172.16.1.1	keelatud	keelatud (C)
5	192.168.3.4	172.16.1.1	keelatud	keelatud (C)
6	192.168.3.4	172.16.6.1	keelatud	keelatud (C)

Reegel B on tegelikult mittevajalik!

Reegel	Saatja	Vastuvõtja	Otsus
A	10.*.*.*	176.16.6.*	OK
C	suva	suva	keelatud

Katsetame (A -> C):

Paketi jrk. Nr.	Saatja	Vastuvõtja	Soovitav otsus	Tegelik otsus (reegel)
1	10.1.99.1	172.16.1.1	keelatud	keelatud (C)
2	10.1.99.1	172.16.6.1	OK	OK (A)
3	10.1.1.1	172.16.6.1	OK	OK (A)
4	10.1.1.1	172.16.1.1	keelatud	keelatud (C)
5	192.168.3.4	172.16.1.1	keelatud	keelatud (C)
6	192.168.3.4	172.16.6.1	keelatud	keelatud (C)