Akademska in raziskovalna mreža Slovenije

Filtri – varnost ali nadloga?

Matjaž Straus
ARNES, Jamova 39, Ljubljana
filtri@arnes.si

Sirikt 2007, Kranjska Gora, 19.4.2007

Filtri – varnost ali nadloga?

- Kaj je filter in kako deluje?
- Kaj pridobimo s filtri?
- Stranski učinki
- "Navodila" za uporabo

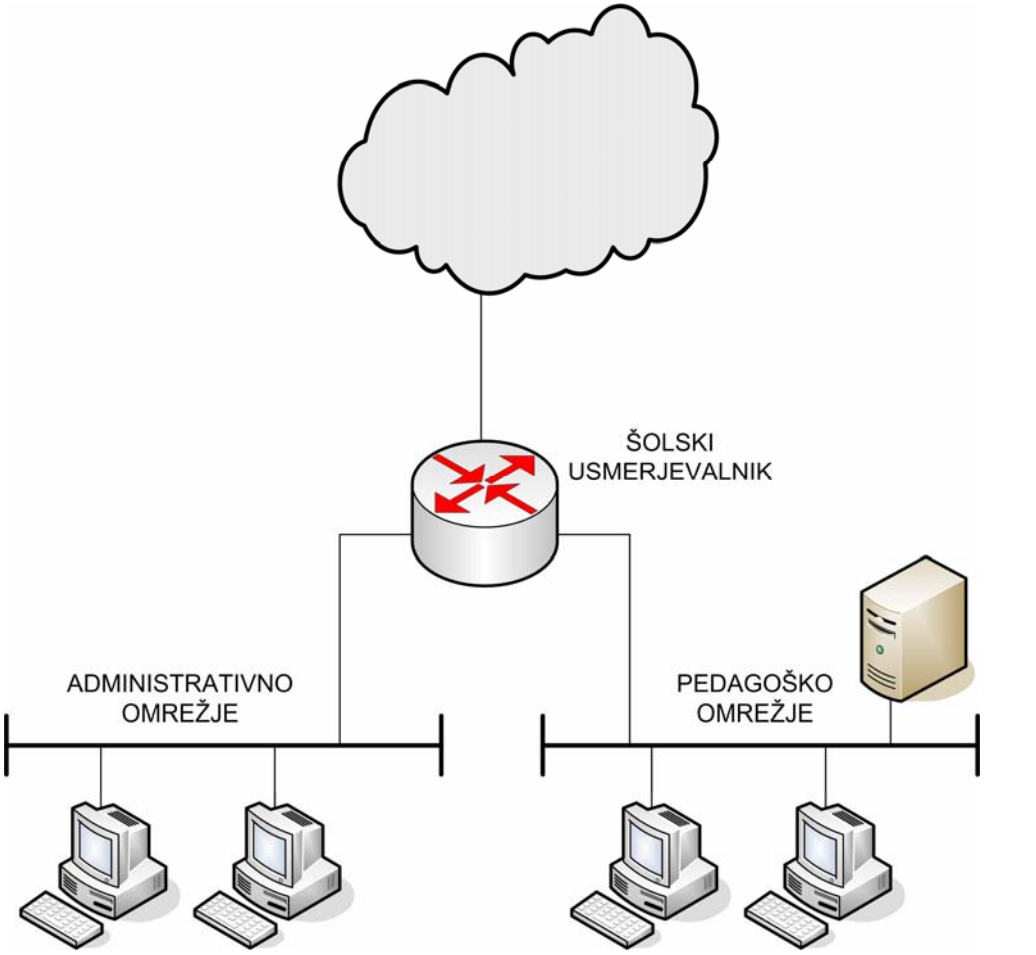
Kaj je filter?

- filter je spisek pravil, ki nadzirajo IP promet skozi usmerjevalnik
- pravila:
  - prepoznavanje IP paketov določenega tipa
  - kaj storiti s takim IP paketom?
    - dovoli in posreduj ga naprej
    - prepovej in zavrzi ga!

    - dodatna možnost: zabeleži ta dogodek v dnevnik

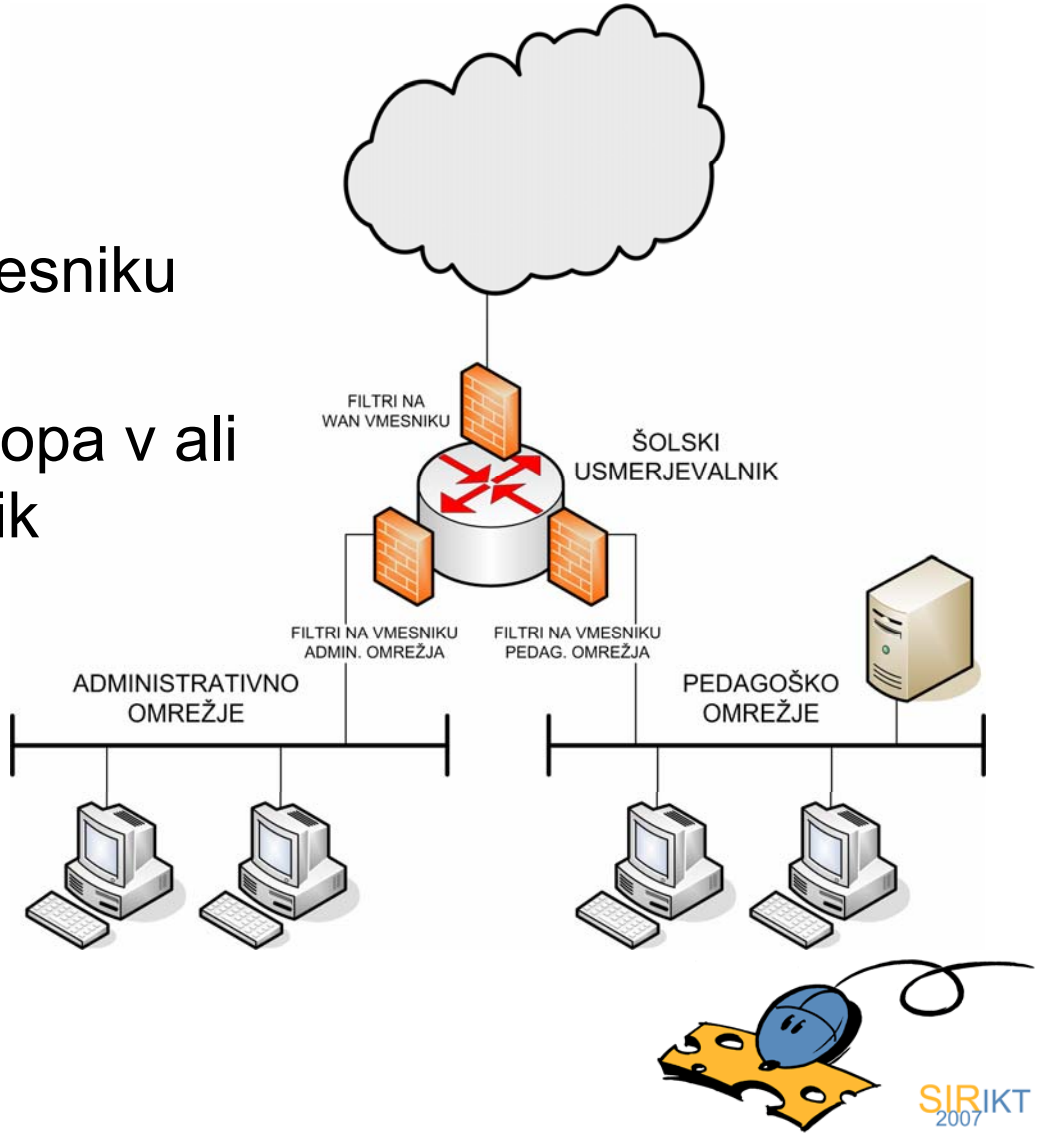
Kaj je filter? (2)

- primer:
  - tipično šolsko omrežje

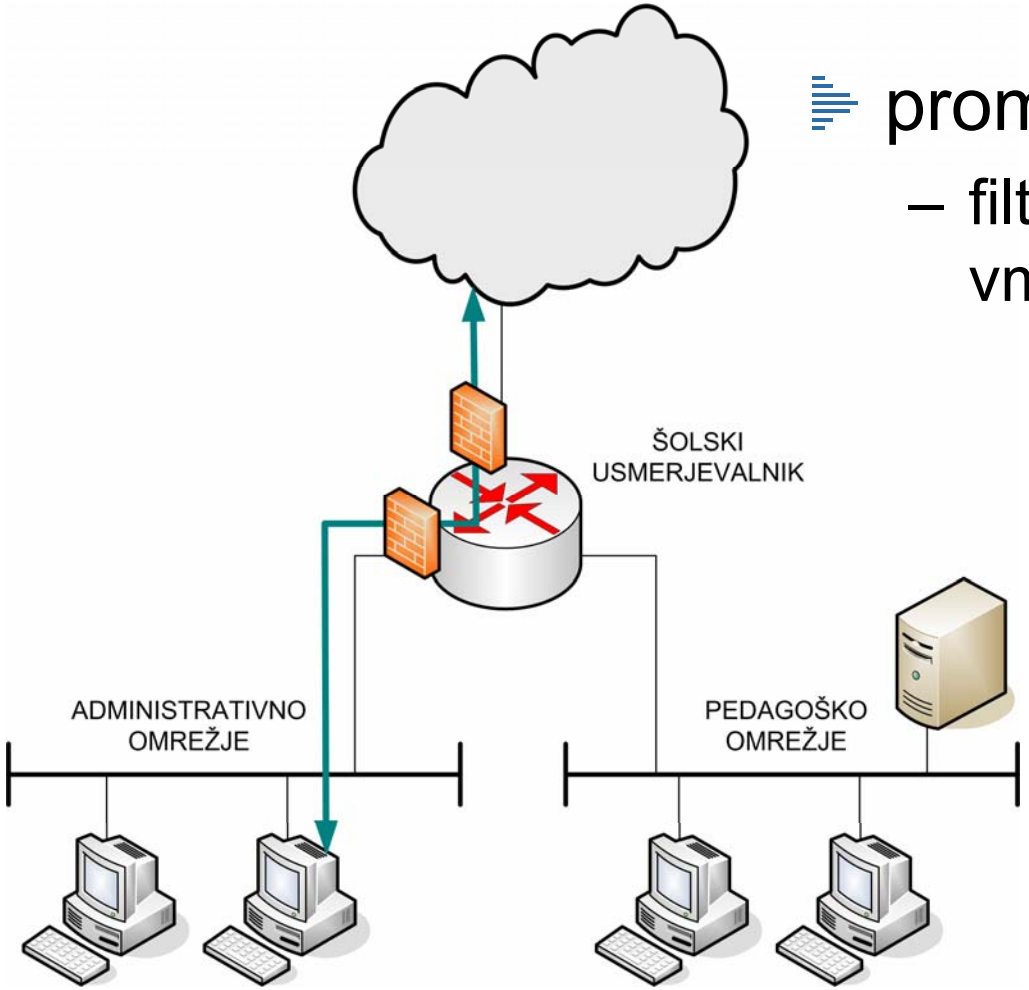


Kaj je filter? (3)

- primer:
  - tipično šolsko omrežje
- filter je aktiven na vmesniku usmerjevalnika
- nadzira promet, ki vstopa v ali zapušča usmerjevalnik

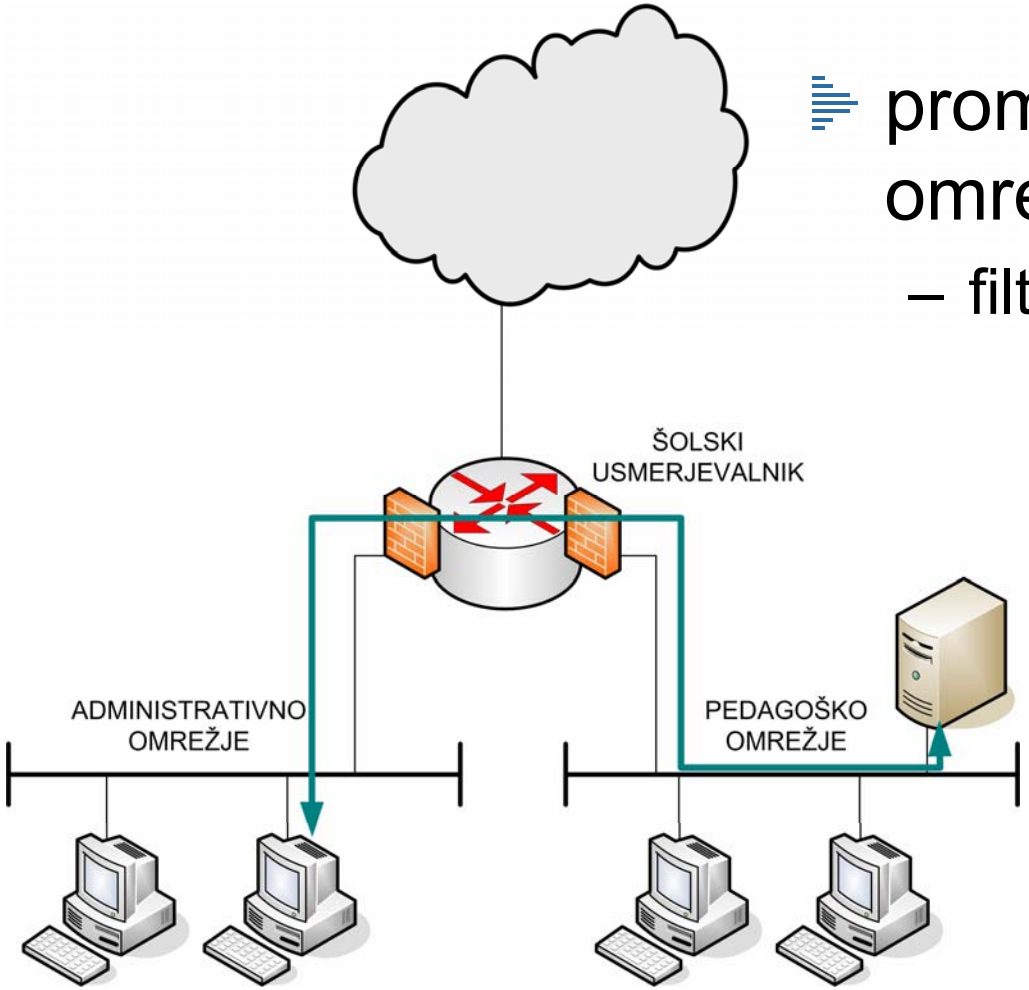


...in kako deluje?



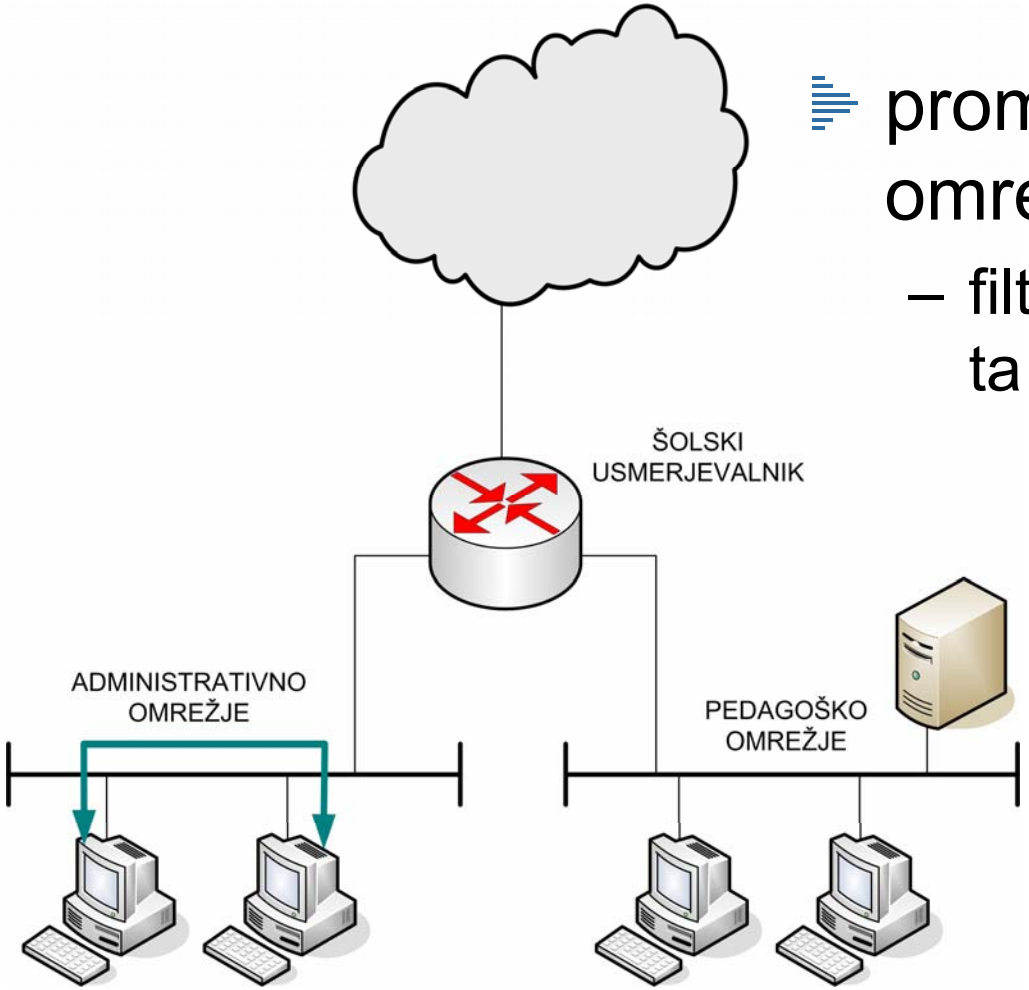
- promet z internetom
  - filtri na WAN in LAN vmesniku

...in kako deluje? (2)



- promet med lokalnima omrežjema
  - filtri na LAN vmesnikih

...in kako deluje? (3)



- promet v lokalnem omrežju
  - filter ne more vplivati na ta promet

...in kako deluje? (4)

- prepoznavanje IP paketa
  - le na podlagi nekaterih informacij v opisu IP paketa in (transportnega) protokola
  - vsebina se ne preglejuje!
  - opis (glava ali "header") IP/TCP paketa
    - IP naslovi (izvor in ponor prometa)
    - IP protokoli (TCP, UDP, ICMP, ...)
    - dodatne lastnosti nekaterih protokolov:
      - TCP/UDP vrata
      - oznaka že vzpostavljene TCP seje
      - ICMP tipi in kode...

...in kako deluje? (4)

- nekega mirnega nedeljskega dopoldneva...

Apr 15 10:47:11: %SEC-6-IPACCESSLOGP: list 112 denied tcp 102.186.107.116(3584) -> 6.3.3.148(139), 1 packet
Apr 15 10:47:14: %SEC-6-IPACCESSLOGP: list 132 denied tcp 196.145.149.193(4398) -> 6.6.6.58(139), 1 packet
Apr 15 10:47:16: %SEC-6-IPACCESSLOGP: list 138 denied tcp 196.145.149.193(4482) -> 6.3.3.7(139), 1 packet
Apr 15 10:47:17: %SEC-6-IPACCESSLOGP: list 132 denied tcp 142.165.108.181(1267) -> 6.6.6.57(139), 1 packet
Apr 15 10:47:18: %SEC-6-IPACCESSLOGP: list 138 denied tcp 142.165.108.181(1917) -> 6.3.3.21(139), 1 packet
Apr 15 10:47:20: %SEC-6-IPACCESSLOGP: list 112 denied tcp 142.165.108.181(1764) -> 6.3.3.167(139), 1 packet
Apr 15 10:47:21: %SEC-6-IPACCESSLOGP: list 150 denied udp 159.105.114.192(123) -> 9.0.5.88(3613), 1 packet
Apr 15 10:47:24: %SEC-6-IPACCESSLOGP: list 132 denied tcp 195.182.167.153(3301) -> 6.6.6.72(80), 1 packet
Apr 15 10:47:25: %SEC-6-IPACCESSLOGP: list 132 denied tcp 196.145.149.193(1120) -> 6.6.6.114(139), 1 packet
Apr 15 10:47:27: %SEC-6-IPACCESSLOGP: list 136 denied tcp 102.186.107.116(3875) -> 6.3.3.86(139), 1 packet
Apr 15 10:47:29: %SEC-6-IPACCESSLOGP: list 132 denied tcp 196.145.149.193(1289) -> 6.6.6.70(139), 1 packet
Apr 15 10:47:30: %SEC-6-IPACCESSLOGP: list 132 denied tcp 195.182.167.153(3402) -> 6.6.6.154(80), 1 packet
Apr 15 10:47:32: %SEC-6-IPACCESSLOGP: list 150 denied udp 159.105.114.192(123) -> 9.0.5.88(3614), 1 packet
Apr 15 10:47:34: %SEC-6-IPACCESSLOGP: list 132 denied tcp 176.135.198.199(4200) -> 6.6.6.176(139), 1 packet
Apr 15 10:47:37: %SEC-6-IPACCESSLOGP: list 132 denied tcp 142.165.108.181(3354) -> 6.6.6.156(139), 1 packet
Apr 15 10:47:41: %SEC-6-IPACCESSLOGP: list 114 denied udp 181.176.191.127(123) -> 2.6.5.36(2049), 1 packet
Apr 15 10:47:43: %SEC-6-IPACCESSLOGP: list 134 denied tcp 142.165.108.181(1852) -> 6.6.6.231(139), 1 packet
Apr 15 10:47:44: %SEC-6-IPACCESSLOGP: list 136 denied tcp 195.182.167.153(3644) -> 6.3.3.111(80), 1 packet
Apr 15 10:47:45: %SEC-6-IPACCESSLOGP: list 114 denied tcp 187.141.177.156(3654) -> 2.6.5.114(11535), 1 packet

- ...in danes – "v živo" na neki šoli

Kaj pridobimo s filtri?

- filtri preprečujejo nezaželjen IP promet
  - zaščita lokalnega omrežja
  - skrb za tuja omrežja – splošno "zdravje" interneta
  - zaščita usmerjevalnika
- filtri odražajo/narekujejo red v lokalnem omrežju

  (v tehniškem svetu malo reda ne škodi)
  - znani strežniki in znane storitve
  - za bolj resne: varnostna politika
- filtri preprečujejo nedovoljen IP promet
  - ponarejeni IP naslovi

Kaj pridobimo s filtri? (2)

- dodatna varnost
  - posebno za sisteme brez protipožarnih pregrad
- omejevanje širjenja internetne "nesnage" (črvi, virusi, spam...)
- preprečevanje nezaželjenega prometa

- onemogočanje zlorab IP naslovnega prostora (*"antispoofing"*)

Filtri in NAT

- Arnes ne nastavlja NAT-a, ker...

	NAT	Javni IP naslovi in filtri
uporaba javnih IP naslovov	**ne**	
računalniki so dosegljivi iz interneta	ne – vsi so skriti za enim javnim IP naslovom	
javni strežniki	**en sam** za določeno storitev	
poljubna neposredna komunikacija (*"end-to-end"*)	**ne**	
vse aplikacije delujejo brez težav	**ne**	
varnost	**osnovna**, podobno kot s filtri	
odkrivanje in odpravljanje težav	**zelo težavno**	
videokonference in QoS	**ne**	
varnostni incidenti	**problemi**	

Filtri in NAT

- Arnes ne nastavlja NAT-a, ker...

	NAT	Javni IP naslovi in filtri
uporaba javnih IP naslovov	**ne**	**da**
računalniki so dosegljivi iz interneta	ne – vsi so skriti za enim javnim IP naslovom	**da**, vendar jih zaščitimo s filtri
javni strežniki	**en sam** za določeno storitev	**da** – ni ovir
poljubna neposredna komunikacija (*"end-to-end"*)	**ne**	**da**, kjer to dovolimo
vse aplikacije delujejo brez težav	**ne**	**da**, če je filter pravilno nastavljen
varnost	**osnovna**, podobno kot s filtri	**osnovna**, več možnosti
odkrivanje in odpravljanje težav	**zelo težavno**	**seveda**!
videokonference in QoS	**ne**	**da**
varnostni incidenti	**problemi**	**lažje** odkrivanje povzročitelja

Stranski učinki

- "Ne dela!"
  - filtri blokirajo promet nekaterih aplikacij, ker te niso pravilno opisane v pravilih
- In kaj sedaj?
  - Izvrtajmo luknjo v filter!
    - Je to res prava pot?
    - Na Arnesu menimo, da **ne**.
  - Posvetujmo se s strokovnjakom, pravilno opišimo problematično aplikacijo in prilagodimo pravila.

Navodila za uporabo

- Ne vrtajte lukenj v filtre!
  - en sam zlorabljen sistem lahko ogrozi celoten segment lokalnega omrežja
- Posvetujte se s strokovnjaki na naslovu filtri@arnes.si
  - natančen opis problematične aplikacije
  - pravilen zapis pravil, ki omočajo IP promet za nemoteno uporabo te aplikacije
  - dodatne nastavitve na usmerjevalniku
  - drug pristop

  - Arnes nudi pomoč pri analizi problema in pomaga pri odpravi težav zaradi filtrov. Luknje so nevarne in niso potrebne!

Nekaj rešljivih "problemov"

- računalniki "se ne vidijo" med seboj
- ne moremo tiskati na tiskalniku v zbornici
- učitelj v učilnici ne more do gradiva na svojem računalniku v kabinetu
- oddaljeni dostop za serviserja
- videkonferenca ne dela
- FTP ne dela
- VPN ne dela

Kaj torej, varnost ali nadloga?

- vsekakor varnost!
- nadloga le:
  - če ne znamo pravilno opisati IP prometa internetne storitve, ki zaradi filtrov ne deluje
  - če ne znamo poiskati druge, varnejše poti
  - če nimamo urejene dokumentacije omrežja

- ne obupajmo in ne vrtajmo lukenj – potrudimo se!
- pomoč nudi skupina filtri@arnes.si