arnes
povezujemo znanje

MREŽA ZNANJA

Ljubljana, 11.–13. oktober 2022

Upravljanje omrežij na VIZ 2022

Filtritranje prometa

Ivan Kolenko

Vsebina

- kaj je filter in delovanje
- protokoli
- primer uporabe v šoli
- koristi filtrov
- težave
- nastavitve
  - zahtevek za odprtje
  - zahtevek ob zlorabi

Osnovni pogoji za zagotovitev varnosti

- fizične ločitve šolskega omrežja od omrežja ARNES in interneta s pomočjo usmerjevalnika
- fizična ločitev administrativnega in pedagoškega dela omrežja
- uporaba varnih internetnih storitev ,
- ustrezna zaščita strežnikov in uporabniških računalnikov.
- filtriranje internetnega prometa

Kaj je filter in delovanje

- Filter je spisek pravil, ki nadzirajo promet skozi usmerjevalnik
- Pravila so namenjena prepoznavanju določene vrste IP (Internet Protokol) paketov
- IP paket prepoznan?
  - Dovolimo (permit) in posredujemo naprej
  - Prepovemo in zavržemo (deny & drop)
    - Zabeleži dogodek v log file zaradi kasnejše analize

Filter – prepoznavanje IP paketa

- IP paket je prepoznan na osnovi nekaterih informacij v opisu IP paketa in transportnega protokola
- Vsebina se NE pregleduje
- Najpogostejši IP protokoli
  - TCP (transmission control protocol)
  - IP (internet protocol)
  - UDP (user datagram protocol)
  - ICMP (internet control message)
  - PIM/IGMP (protocol independent multicast)
- Seveda je spisek internetnih protokolov bistveno daljši in si ga lahko ogledamo tukaj

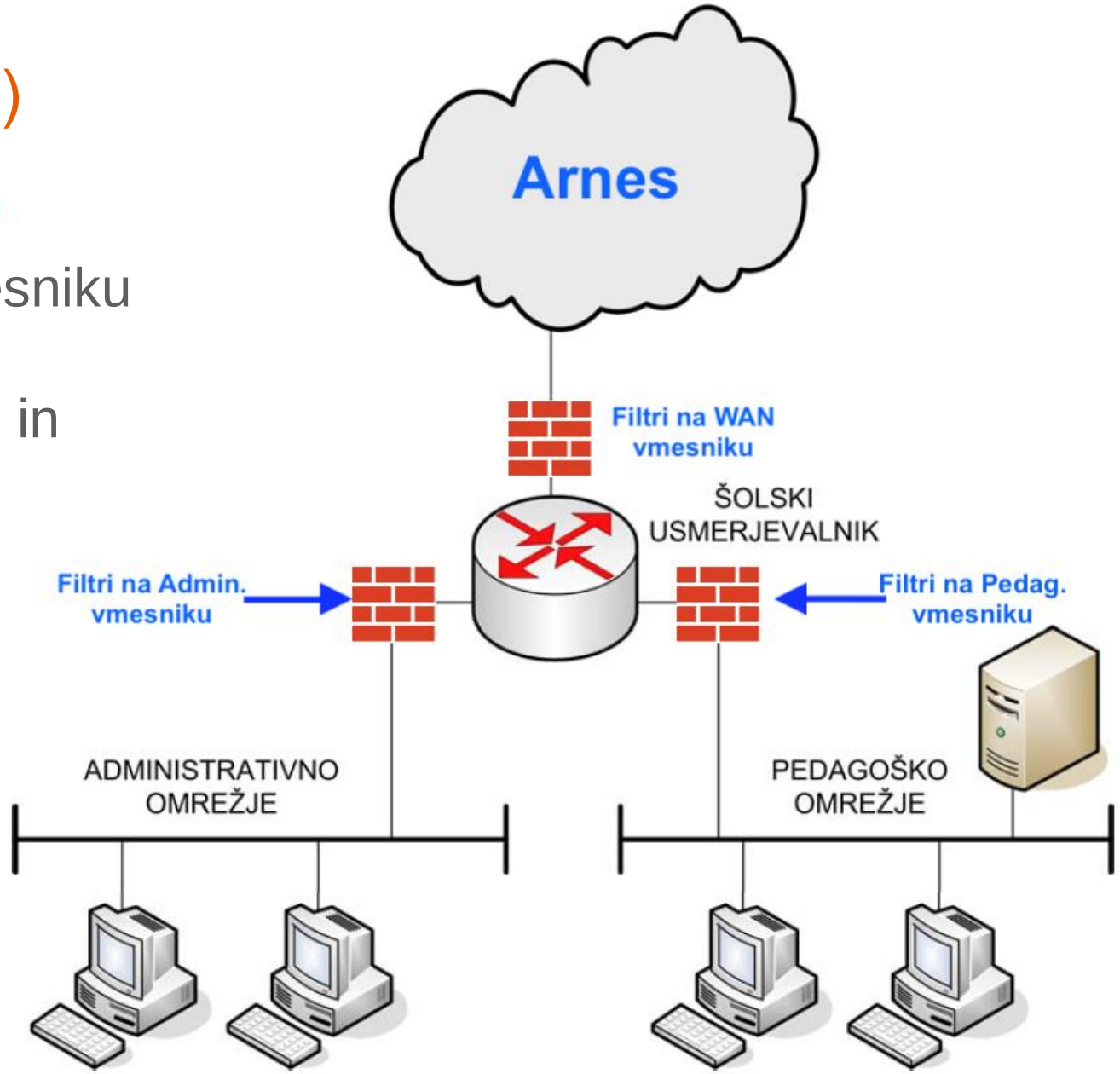
Filter – protokoli

Razen IP protokola so definirani še drugi podatki – TCP/UDP vrata (port number) , ICMP tipi in kode ***Najpogostje uporabljani porti:***

20: File Transfer Protocol (FTP) Data Transfer
21: File Transfer Protocol (FTP) Command Control
22: Secure Shell (SSH) Secure Login
23: Telnet remote login service, unencrypted text messages
25: Simple Mail Transfer Protocol (SMTP) E-mail routing
53: Domain Name System (DNS) service
80: Hypertext Transfer Protocol (HTTP) used in the World Wide Web
110: Post Office Protocol (POP3)
119: Network News Transfer Protocol (NNTP)
123: Network Time Protocol (NTP)
143: Internet Message Access Protocol (IMAP) Management of digital mail
161: Simple Network Management Protocol (SNMP)
194: Internet Relay Chat (IRC)
443: HTTP Secure (HTTPS) HTTP over TLS/SSL

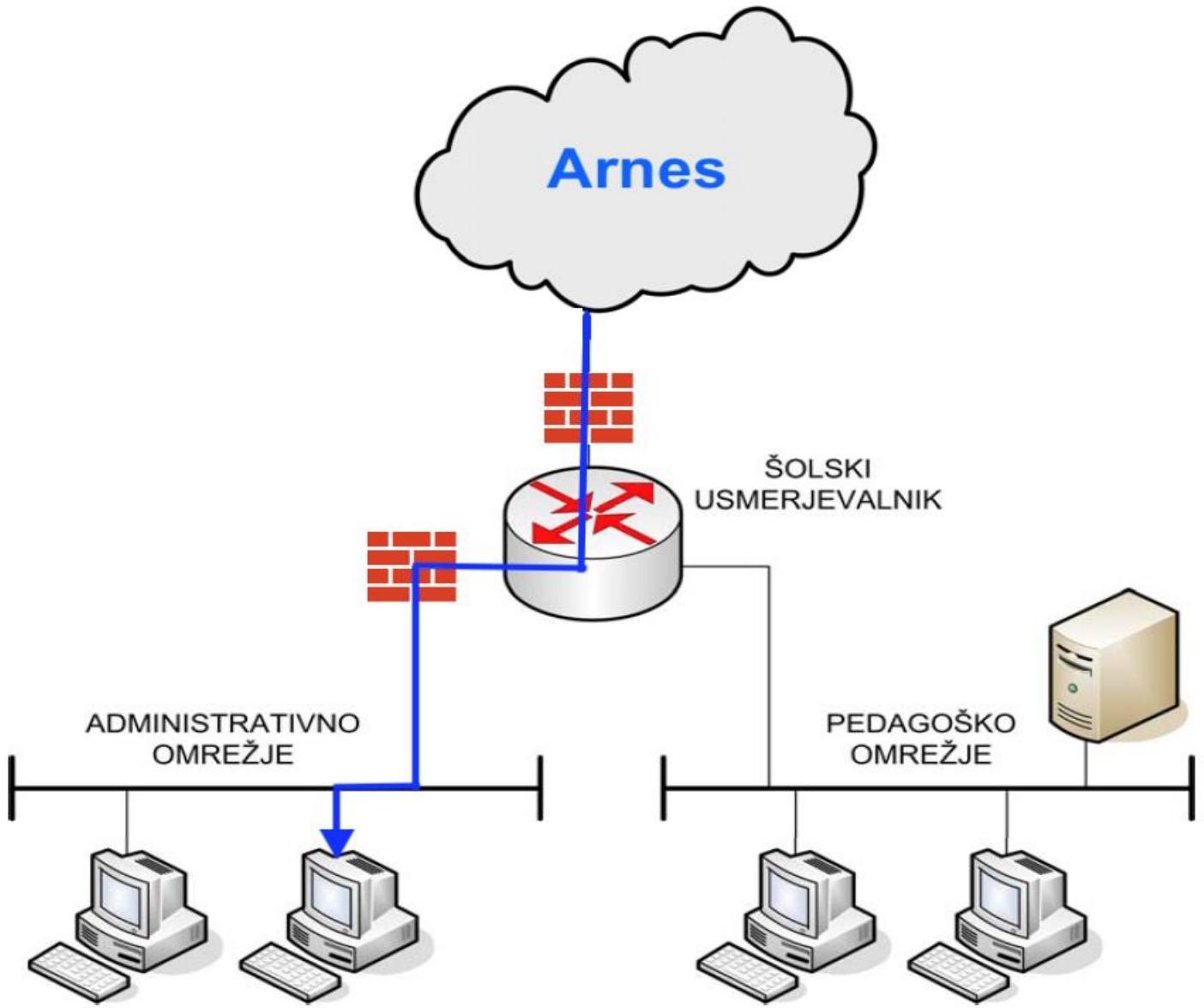
Primer uporabe v šoli (1)

- Filter aktiven na WAN vmesniku
- Nadzor prometa ob vstopu in izhodu iz routerja



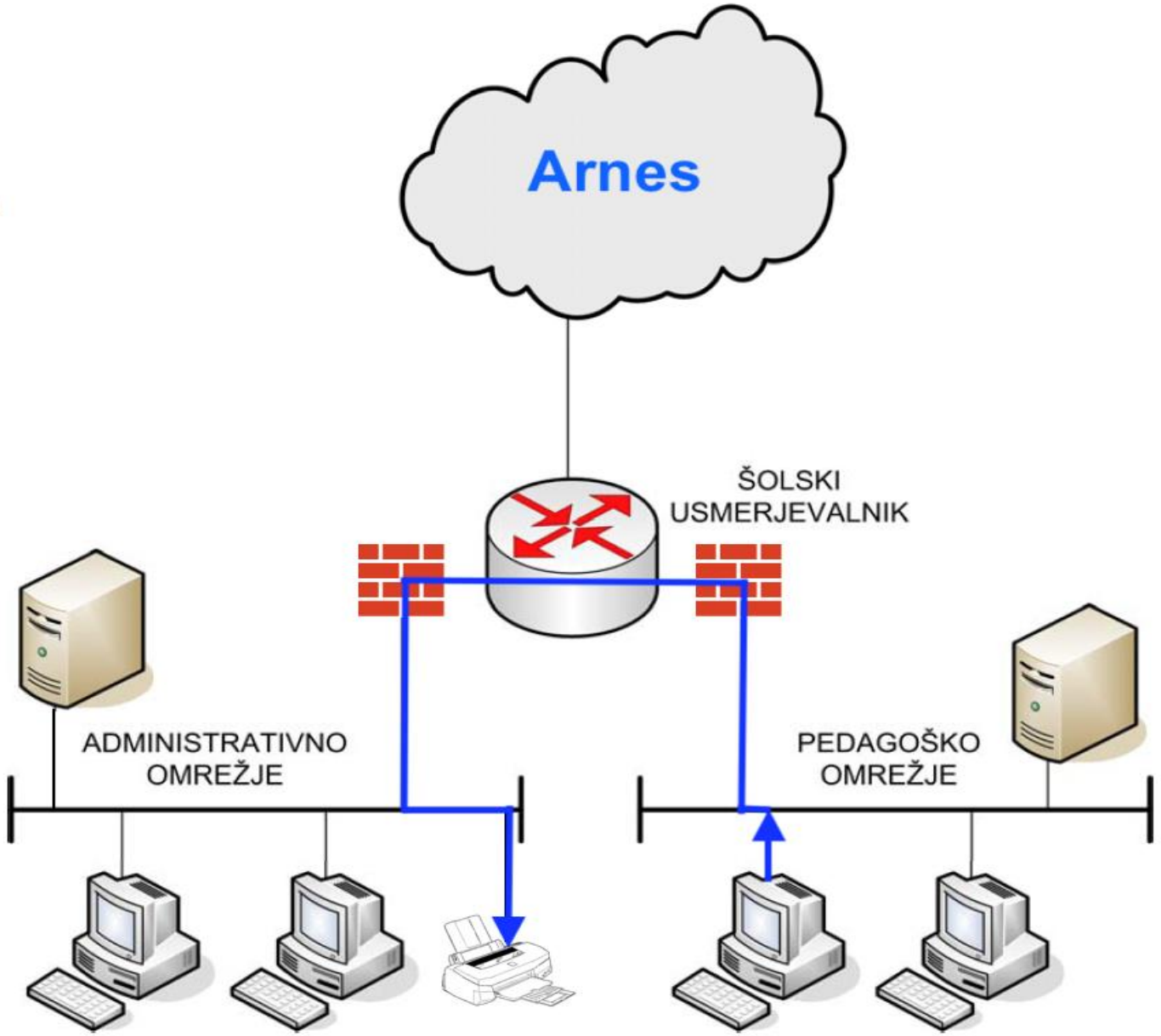
Primer uporabe v šoli (2)

- Dostop do interneta
  - Filtri na WAN in LAN vmesniku



Primer uporabe v šoli (3)

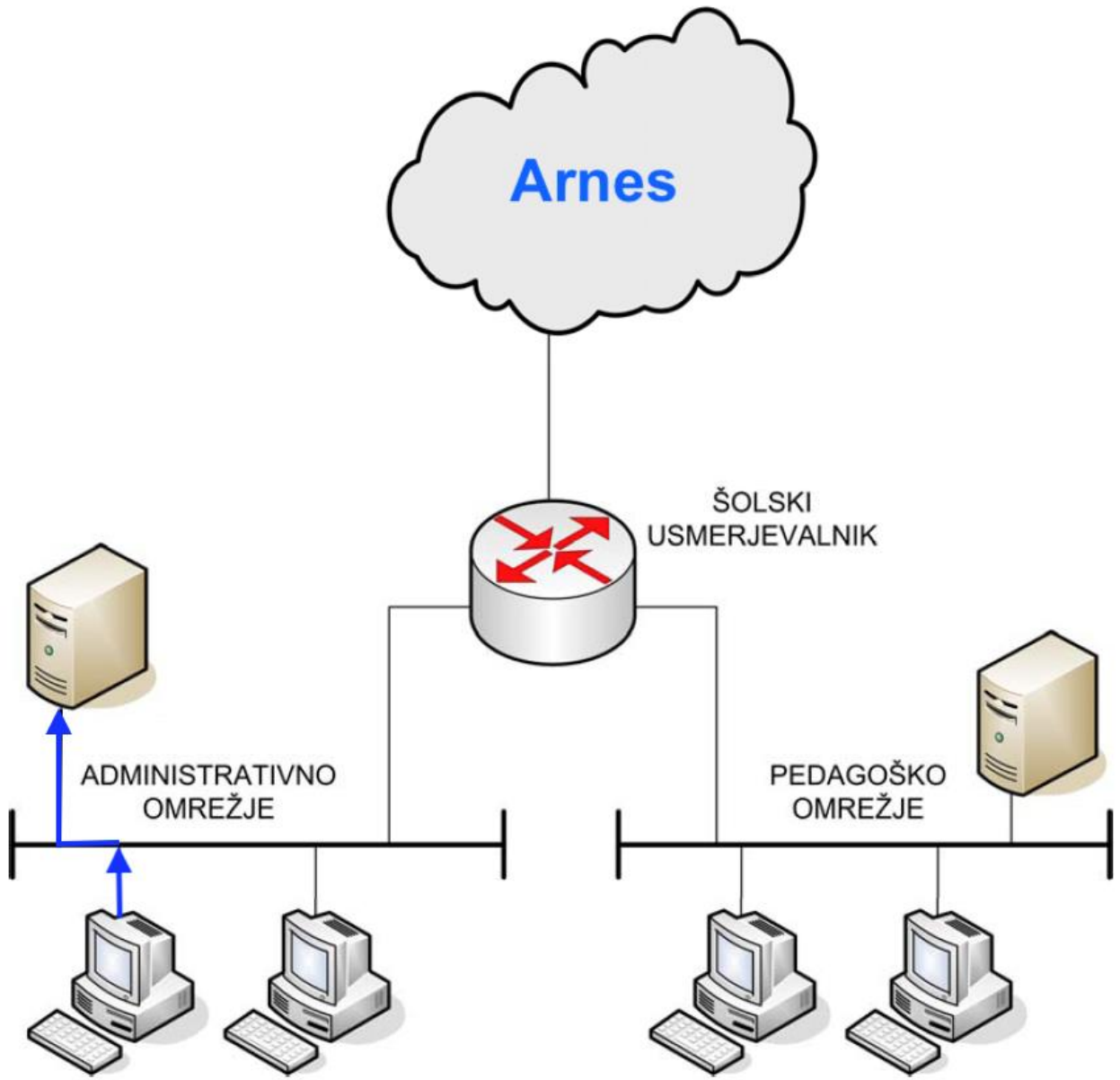
- Tiskanje iz Pedagoškega v Administrativno omrežje
- Filtri na LAN vmesnikih



Primer uporabe v šoli (4)

- Promet v lokalnem omrežju
- Filtri Arnes ne morejo vplivati na ta promet

Za strežnike v lokalnem omrežju moramo poskrbeti sami!!



Filter – koristi

- Preprečevanje nezaželjenega IP prometa
  - Zaščita šolskega omrežja
  - Zaščita tujega omrežja – iskoriščanje omrežja za napade na druga omrežja (primer v nadaljevanju)
  - Zaščita usmerjevalnika
- Preprečevanje nedovoljenega prometa
  - Ponarejeni IP naslovi
  - onemogočanje zlorab IP naslovov (Antispoofing)
  - Omejevanje širjenja virusov, spam-a,..
- Osnovno varovanje sistemov brez požarnih zidov (FireWall)
  - …

NAT (Network Address Translation) -da/NE

	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

Filtri – težave

- Blokiranje določenih aplikacij, ker niso v skladu z opisanimi pravili
- Za VSAK prehod iz enega v drugo omrežje(Administrativno/Pedagoško) je potrebno ustrezno nastaviti filtre
  - Dostop do sistemskega tiskalnika
  - Dostop do določenega strežnika
  - Uporaba določene aplikacije ..
  - …

Filtri - nastavitve

- V osnovi so filtri na usmerjevalnikih Arnes **NASTAVLJENI!**
- Za spremembo oz. dopolnitev filtra/filtrov se je potrebno posvetovati s strokovnjaki ARNES (filtri@arnes.si)
- Zahtevek za spremembo natančno definiramo (primer na koncu)
- Zahtevek za spremembo filtrov lahko poda le pooblaščena oseba na šoli!

Filtri – nastavitve (2)

- Tiskalnik v zbornici ni “viden” iz učilnice
- Učitelj v razredu ne vidi gradiv na računalniku v kabinetu
- Serviser potrebuje oddaljen dostop
- FTP ne deluje
- Videokonferenca ne deluje
- VPN ne deluje

Filtri – nastavitve – primer zahtevka

Serviserju želimo omogočiti SSH dostop do strežnikov

– komunikacija Arnes filtri – ROID:

od:	**ROID**<ime,priimek@sola.si>
za:	Filtri ARNES <filtri@arnes.si>
datum:	x.xxx. 2016 11:26
zadeva:	Sprememba filtrov za sola.si

Za potrebe serviserja strežnikov prosim za odprtje dostopov
iz IP-ja **xxx.xxx.8.43** (IP serviserja) do naslednjih IP-jev (strežniki, NAS-i, ..)

- **SSH dostop port 22**:

1.) strežniki:

xxx.xx.xxx.109 , xxx.xx.xxx.110, xxx.xx.xxx.111, xxx.xx.xxx.112 , xxx.xx.xxx.113,
xxx.xx.xxx.115, xxx.xx.xxx.117, xxx.xx.xxx.208, xxx.xx.xxx.211,

Odgovor Arnes-a

Urejeno.

+ permit tcp host xxx.xxx.8.43 host xxx.xx.xxx.109 eq 22
+ permit tcp host xxx.xxx.8.43 host xxx.xx.xxx.110 eq 22
+ permit tcp host xxx.xxx.8.43 host xxx.xx.xxx.111 eq 22
+ permit tcp host xxx.xxx.8.43 host xxx.xx.xxx.112 eq 22
+ permit tcp host xxx.xxx.8.43 host xxx.xx.xxx.113 eq 22
+ permit tcp host xxx.xxx.8.43 host xxx.xx.xxx.115 eq 22
+ permit tcp host xxx.xxx.8.43 host xxx.xx.xxx.117 eq 22
+ permit tcp host xxx.xxx.8.43 host xxx.xx.xxx.208 eq 22
+ permit tcp host xxx.xxx.8.43 host xxx.xx.xxx.211 eq 22

ARNES

V primeru nadaljnega dopisovanja na isto tematiko zadrzite trenutni izpis v polju Zadeva/Subject: [ARNES #stevilka]

Filtri – primer ukrepanja - obvestilo

- Izkoriščanje omrežja za napade na druga omrežja
  - SICERT pošlje obvestilo o možni zlorabi:

========== SICERT mail ==========
Prejeli smo obvestilo o možni zlorabi naprave z IP naslovom xxx.xxx.xxx.xxxx,
ki se po naših podatkih nahaja v vašem omrežju, in naj bi bila uporabljena
v DNS napadih z odbojem (angl. "DNS reflection", tudi "DNS amplification").
Več o samem napadu si lahko preberete v našem članku:

https://www.cert.si/vrnitev-odpisanih/

spodaj je izsek izpiska prometa.

> 2016-03-02 06:22:45.123738 IP (tos 0x0, ttl 108, id 4309, offset 0,
> flags [DF], proto UDP (17), length 1233) xxx.xxx.xxx.xxxx.53 >
> xxx.xxx.xxx.xxxx.46551: 9814| 11/0/1 someone.gov A xxx.xxx.xxx.xxxx, someone.gov
> NS[|domain]
> 0x0000: 4500 04d1 10d5 4000 6c11 ce48 c102 327b E.....@.l..H..2{
> 0x0010: 4297 f4e9 0035 b5d7 04bd 7dbe 2656 8380 B....5....}.&V..
> 0x0020: 0001 000b 0000 0001 0463 7073 6303 676f .....someone.go
> 0x0030: 7600 00ff 0001 c00c 0001 0001 0000 31a8 v.....1.
> 0x0040: 0004 3f4a 6d02 c00c 0002 0001 0000 31a8 ..?Jm.....1.
> 0x0050: 0012 ..
> 2016-03-02 06:22:45.123812 IP (tos 0x0, ttl 108, id 4310, offset 0,
.....

Filtri – primer ukrepanja - Ukrepanje

Ukrepanje:

Mail na filtri@arnes.si da se omeji zunanji dostop do strežnika

Filtri – primer izpisa

Naloga:

Pridobiti
trenutno stanje filtrov
in jih pregledati/urediti

```
ssola_pedag_gw1123.123.123.100-out
anti-spoofing
network 123.123.123.0/25   network 123.123.123.0/25 *                    permit    anti-spoofing
network 123.123.123.0/25   network 123.123.123.128/26      *              permit    anti-spoofing
network 123.123.123.128/26      network 123.123.123.0/25    *             permit    anti-spoofing
network 123.123.123.128/26      network 123.123.123.128/26 *              permit    anti-spoofing
network 123.123.123.128/25      network 123.123.123.0/25    *             permit    anti-spoofing
network 123.123.123.128/25      network 123.123.123.128/25 *              permit    anti-spoofing
network 123.123.123.0/25   any  *                          deny     LOG
network 123.123.123.128/26      any  *                         deny     LOG
DNS, NTP and ICMP
any             network 123.123.123.128/25   UDP   53      >1023       permit    DNS for LAN's
any             network 123.123.123.0/25     UDP   53      137      permit    netbios-ns
any             network 123.123.123.128/26   UDP   53      137      permit    netbios-ns
any             network 123.123.123.128/25   ICMP  type/code 0      permit    permitted ICMP messages
any             network 123.123.123.0/25     ICMP  type/code 3/1       permit    permitted ICMP messages
any             network 123.123.123.0/25     ICMP  type/code 11     permit    permitted ICMP messages
any             network 123.123.123.128/25   ICMP  type/code 3/13       permit    permitted ICMP messages
any             network 123.123.123.128/25   UDP   123     >1023       permit    NTP
any             network 123.123.123.128/25   UDP   123     123      permit
TCP established
any             network 123.123.123.0/25     TCP             established    permit    TCP established
any             network 123.123.123.128/26   TCP             established    permit    TCP established
any             network 123.123.123.128/25   TCP             established    permit    TCP established
servers
any             123.123.123.115   UDP 68    67          permit    DHCP requests
xxx.xxx.xx.66   123.123.123.115   UDP                   permit    Upstream radius promet
xx.xx.xx.141    123.123.123.115   UDP                   permit    Upstream radius promet
network xx.xx.xx.xx/26      123.123.123.115   *                   permit    dovoljen ves promet
any             123.123.123.123   UDP       53          deny      blokiraj DNS xx.xx.2016
any             123.123.123.123   TCP       53          deny      blokiraj DNS xx.xx.2016
any             123.123.123.123   UDP       >1023       deny      blokiraj DNS xx.xx.2016
```

Vprašanja

Odgovori