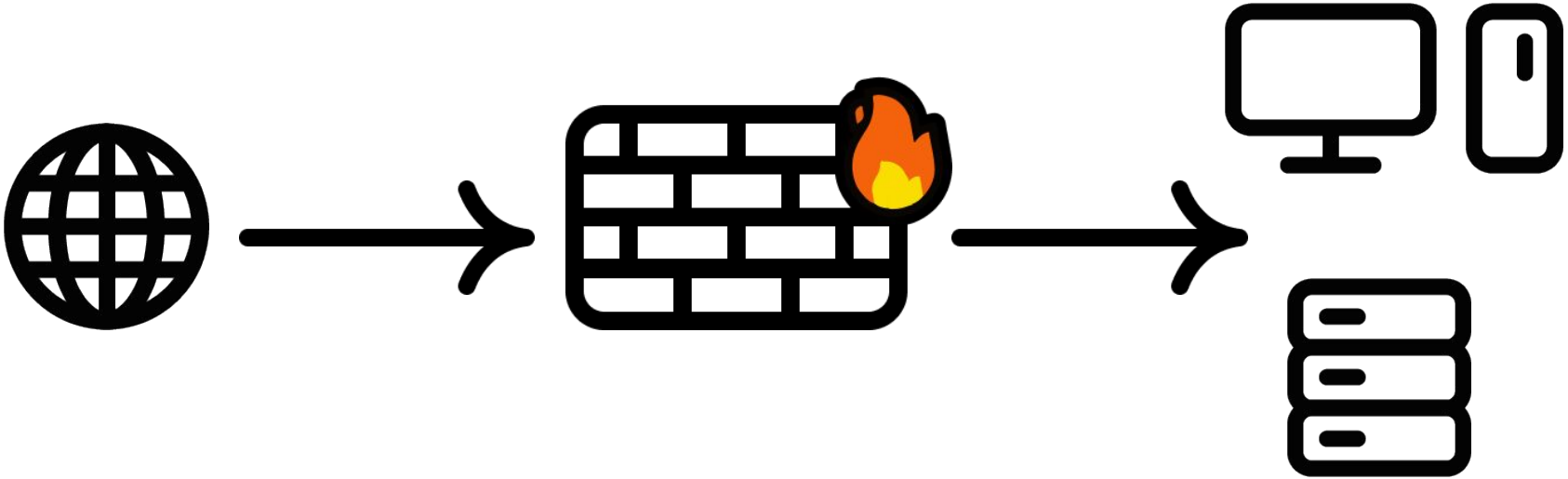
L7 firewall založený na Linuxe
(Linux Based L7 Firewall)

Terézia Kabátová

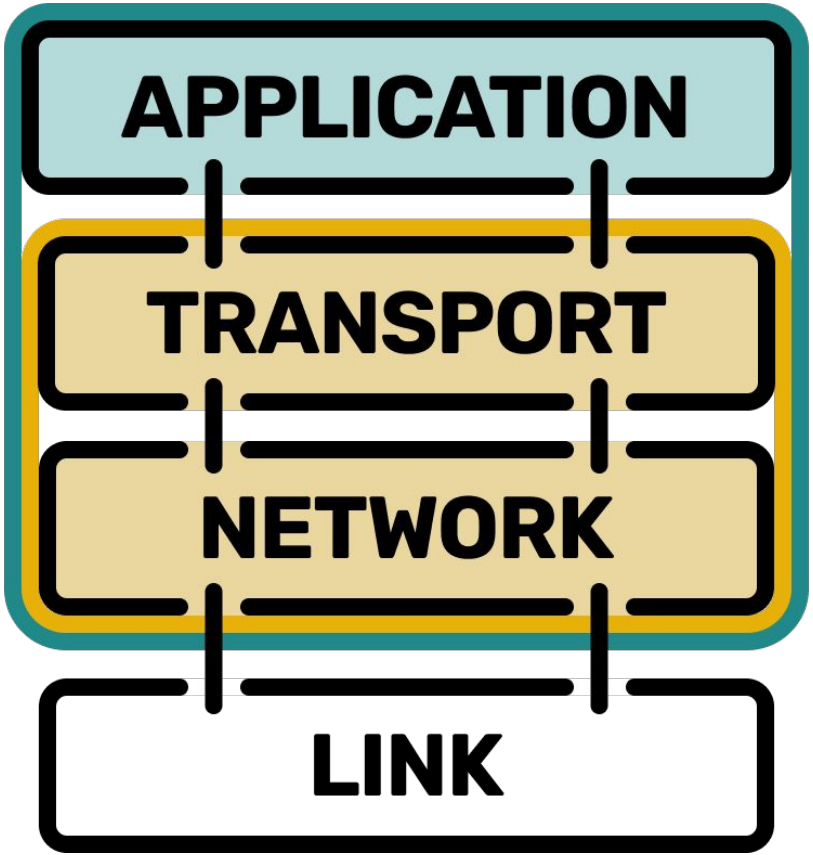
školiteľ: RNDr. Jaroslav Janáček, PhD.

FIREWALL



APLIKAČNÝ (L7) FIREWALL

KLASICKÝ FIREWALL



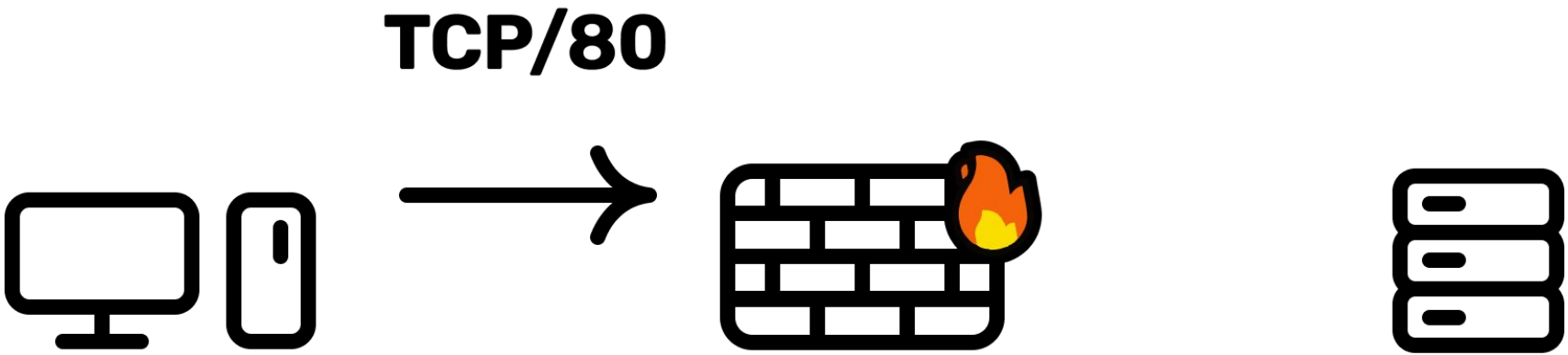
V ČOM JE ROZDIEL?

FUNKCIONALITA L7 FIREWALLU

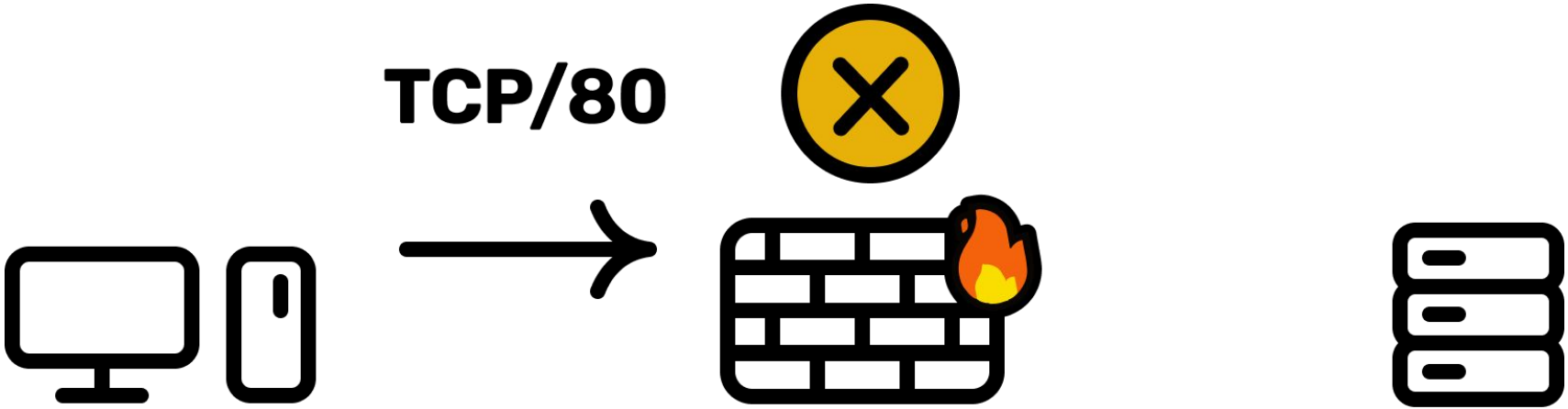
VALIDÁCIA L7 PROTOKOLOV

- porovnanie L7 dát s definíciou protokolu
- umožňuje blokovanie prístupu do siete daným L7 protokolom

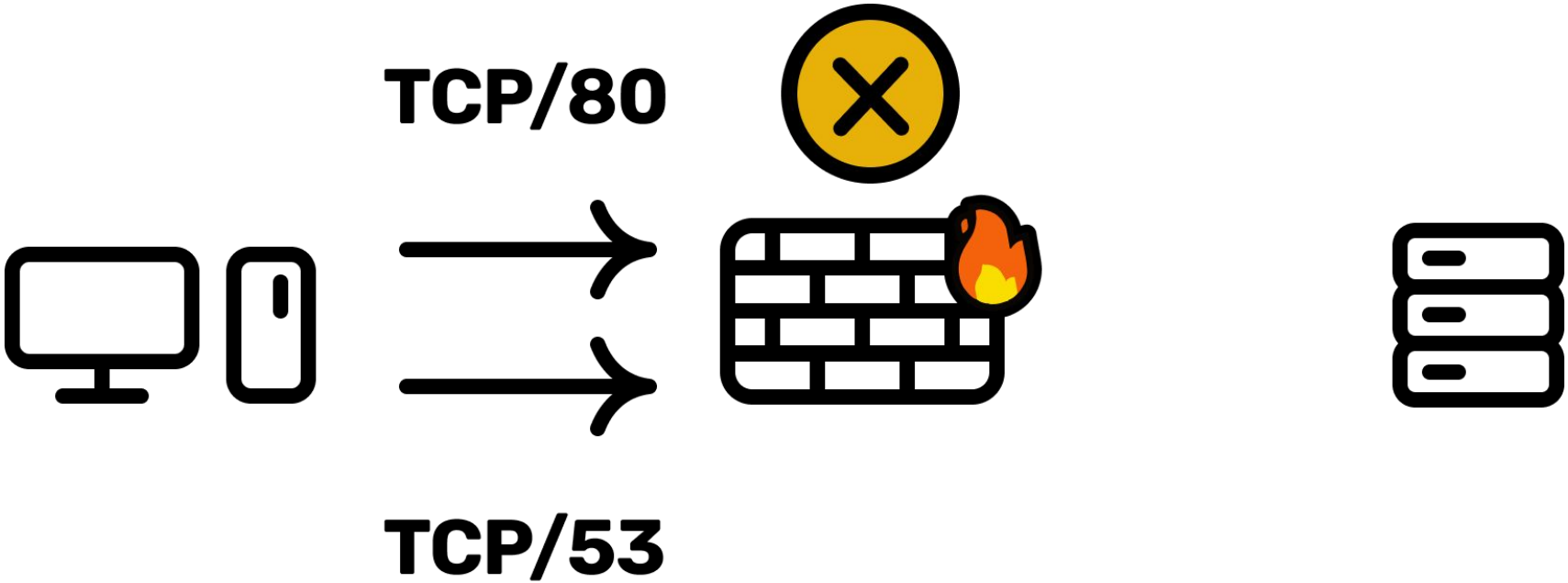
VALIDÁCIA L7 PROTOKOLOV



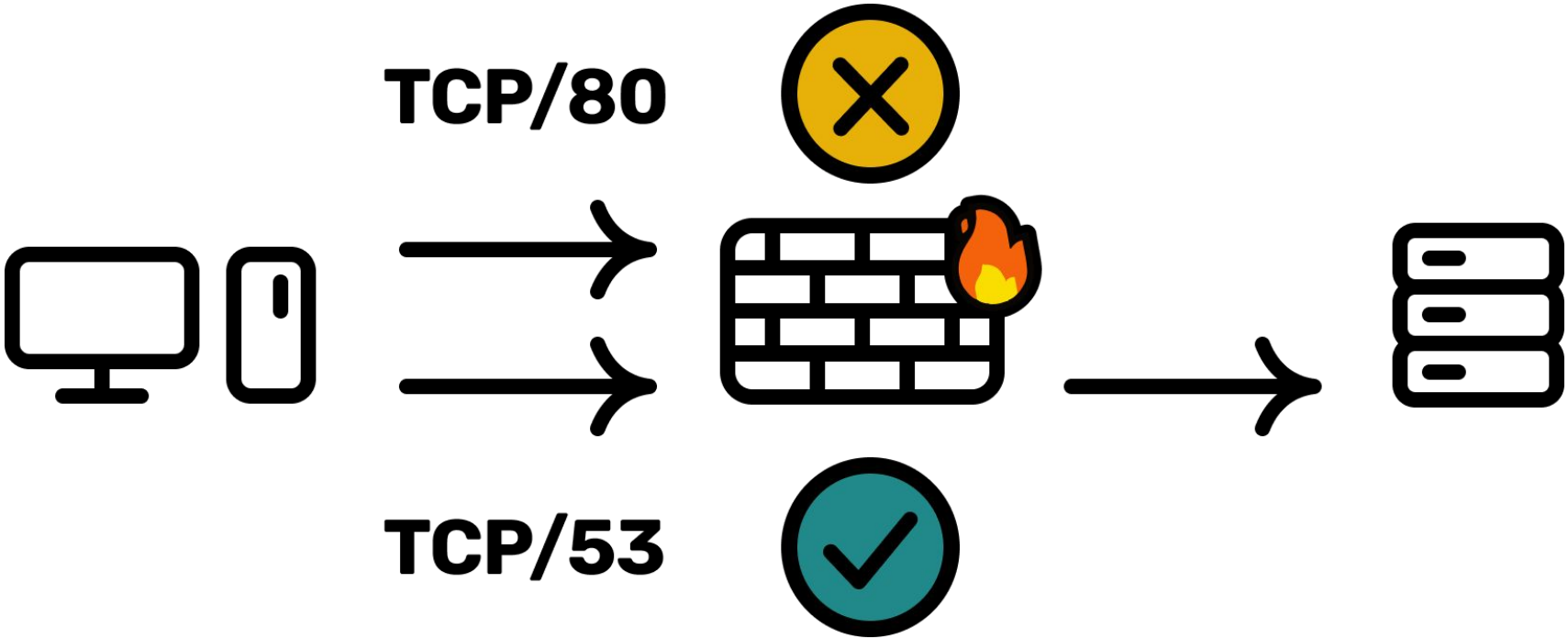
VALIDÁCIA L7 PROTOKOLOV



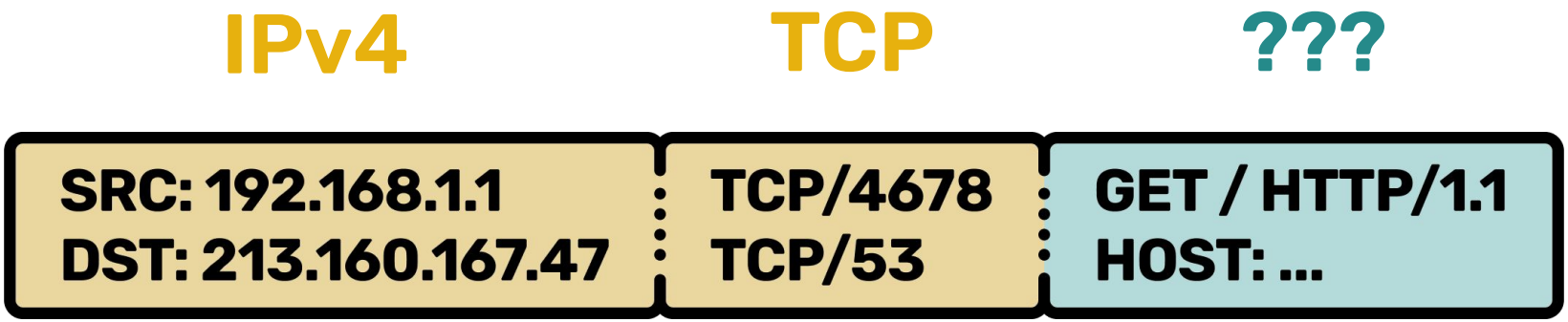
VALIDÁCIA L7 PROTOKOLOV



VALIDÁCIA L7 PROTOKOLOV

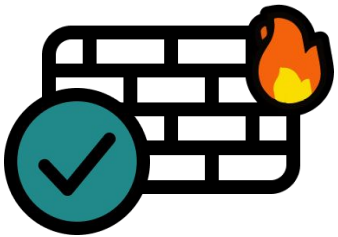


VALIDÁCIA L7 PROTOKOLOV



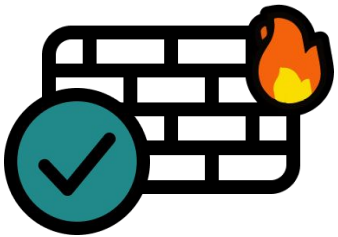
VALIDÁCIA L7 PROTOKOLOV

IPv4	TCP	???
SRC: 192.168.1.1 DST: 213.160.167.47	TCP/4678 TCP/53	GET / HTTP/1.1 HOST: ...



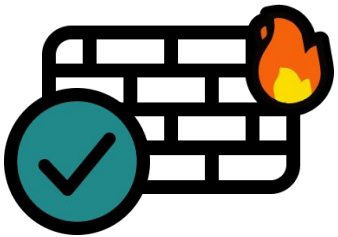
VALIDÁCIA L7 PROTOKOLOV

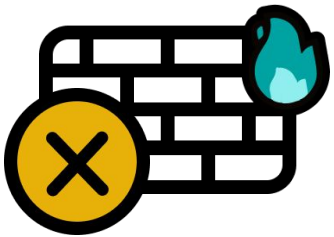
IPv4	TCP	HTTP
SRC: 192.168.1.1 DST: 213.160.167.47	TCP/4678 TCP/53	GET / HTTP/1.1 HOST: ...



VALIDÁCIA L7 PROTOKOLOV

IPv4	TCP	HTTP
SRC: 192.168.1.1 DST: 213.160.167.47	TCP/4678 TCP/53	GET / HTTP/1.1 HOST: ...

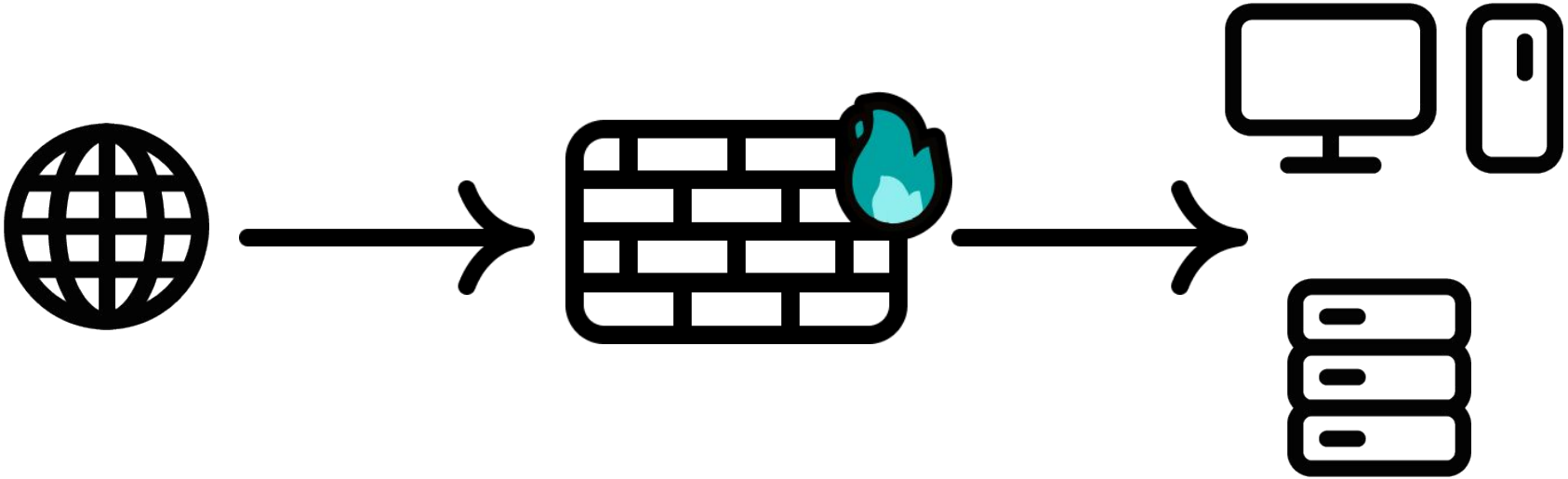




ANALÝZA KOREKTNÝCH L7 SPRÁV

- správa zodpovedá protokolu
- administrátor môže špecifikovať dodatočné podmienky
  - drop uri STR match '.*wp-admin.*';

L7 FIREWALL



EXISTUJÚCE RIEŠENIA

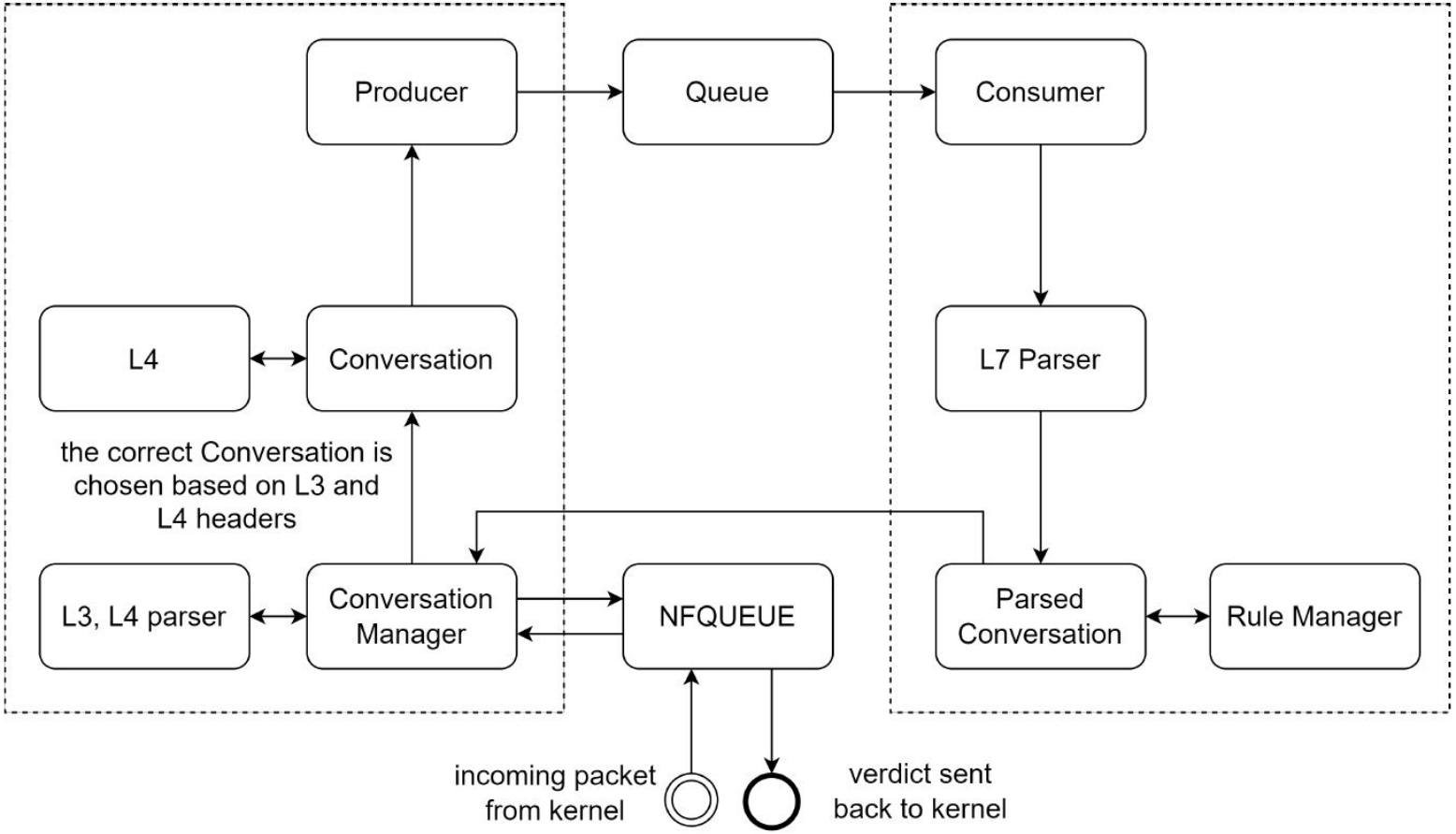
- príliš úzke zameranie – WAF
- nezodpovedajú definícii firewallu – IDS/IPS
- vysoká cena – Cisco, Palo Alto, ...

VÝSLEDKY

IMPLEMENTÁCIA A TESTOVANIE

IMPLEMENTÁCIA

- funkcionalita
  - validácia L7 protokolov
  - analýza korektných správ
- HTTP a DNS

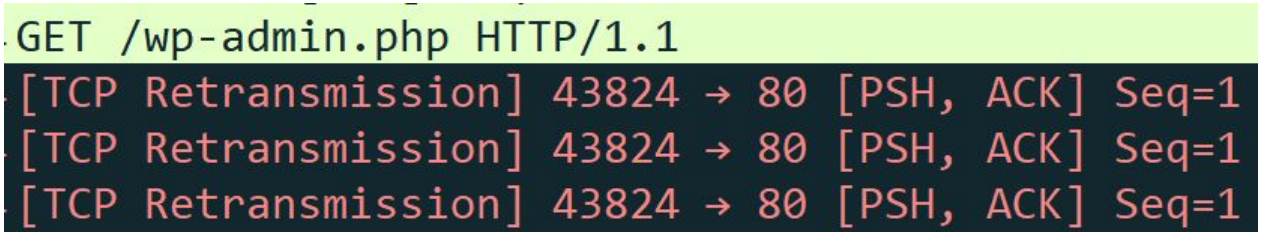

Producer
Queue
Consumer
L4
Conversation
L7 Parser
the correct Conversation is chosen based on L3 and L4 headers
L3, L4 parser
Conversation Manager
NFQUEUE
Parsed Conversation
Rule Manager
incoming packet from kernel
verdict sent back to kernel

TESTOVANIE FUNKČNOSTI

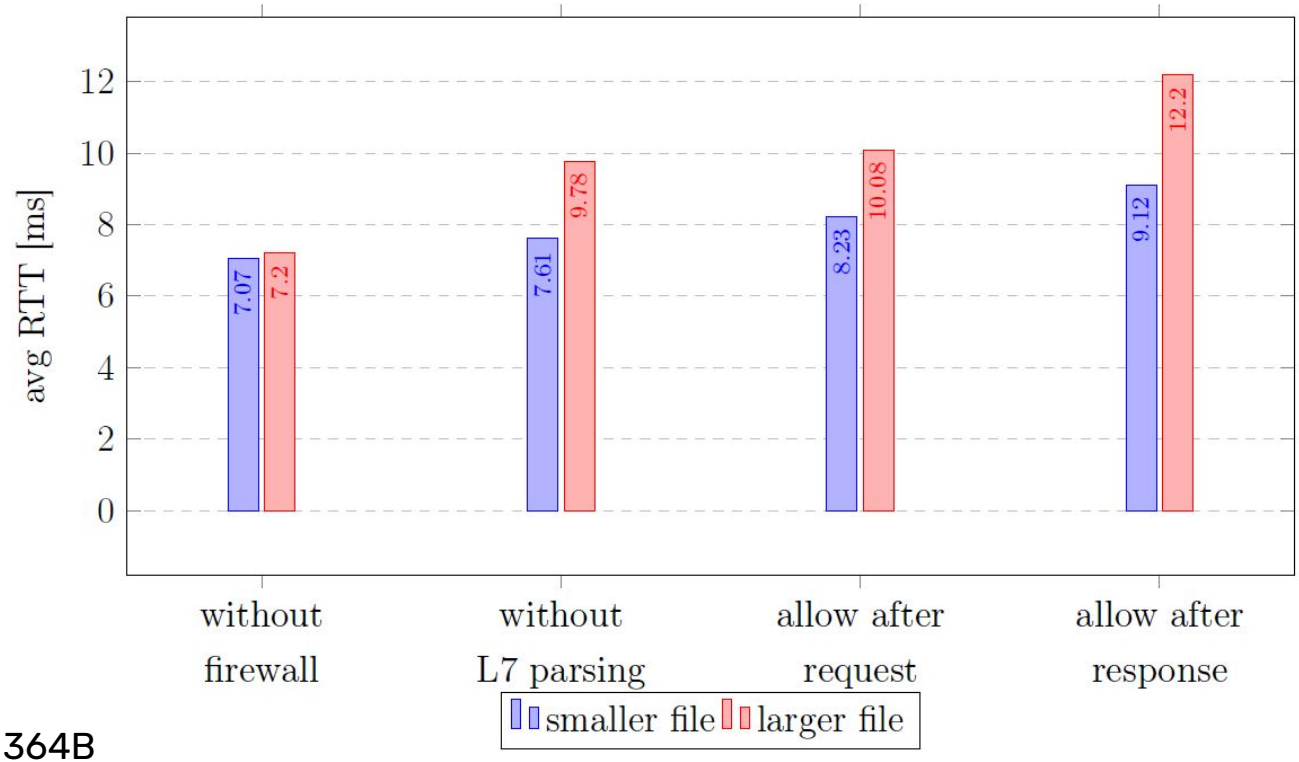
- testovacie scenáre navrhnuté podľa útokov na HTTP a DNS
- vyhodnotené na základe odchytených paketov pred a za firewallom

ZÁKAZ PRÍSTUPU K ADMIN ROZHRANIU

drop uri STR match '.*wp-admin.*';

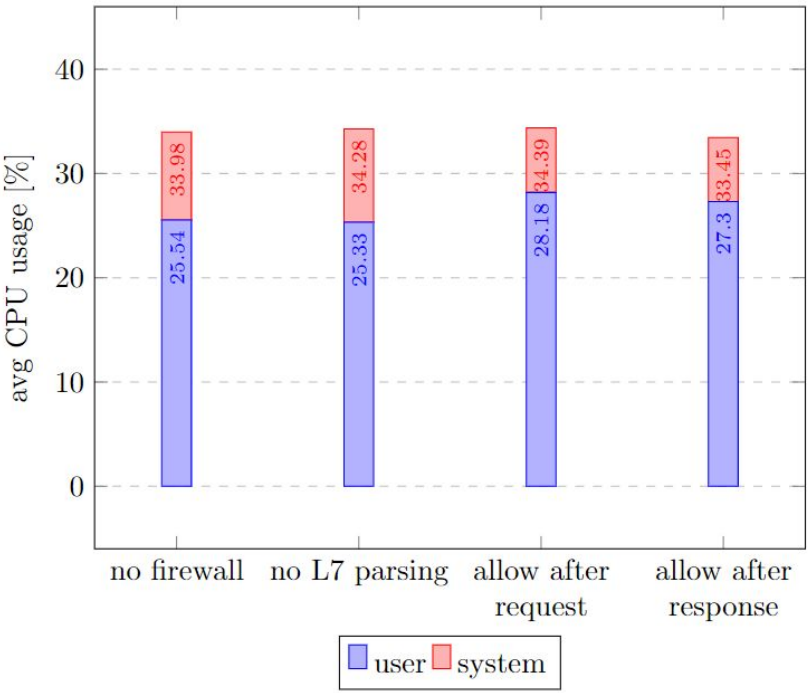


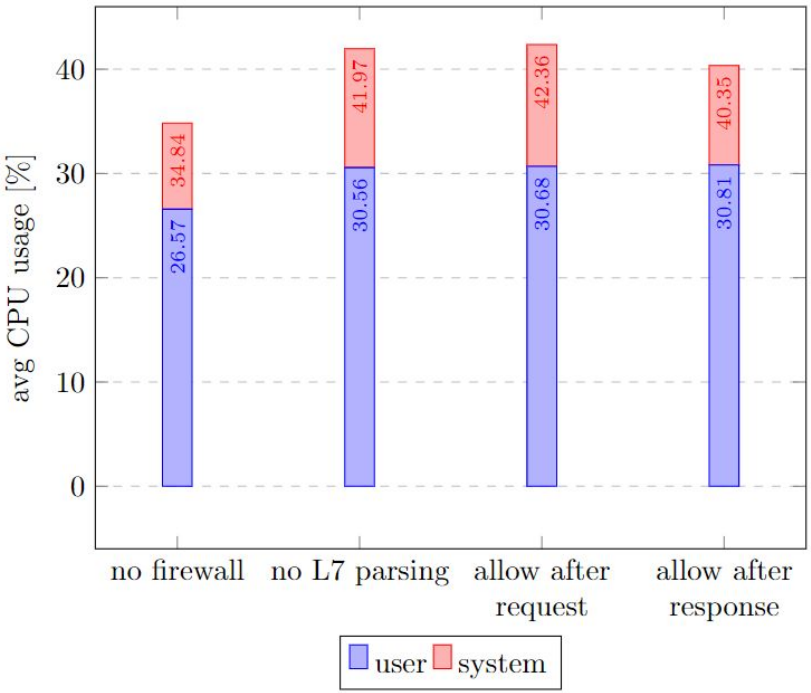
TESTOVANIE VÝKONU - RTT



smaller file – 364B
larger file – 53,2KB

TESTOVANIE VÝKONU - VYUŽITIE CPU





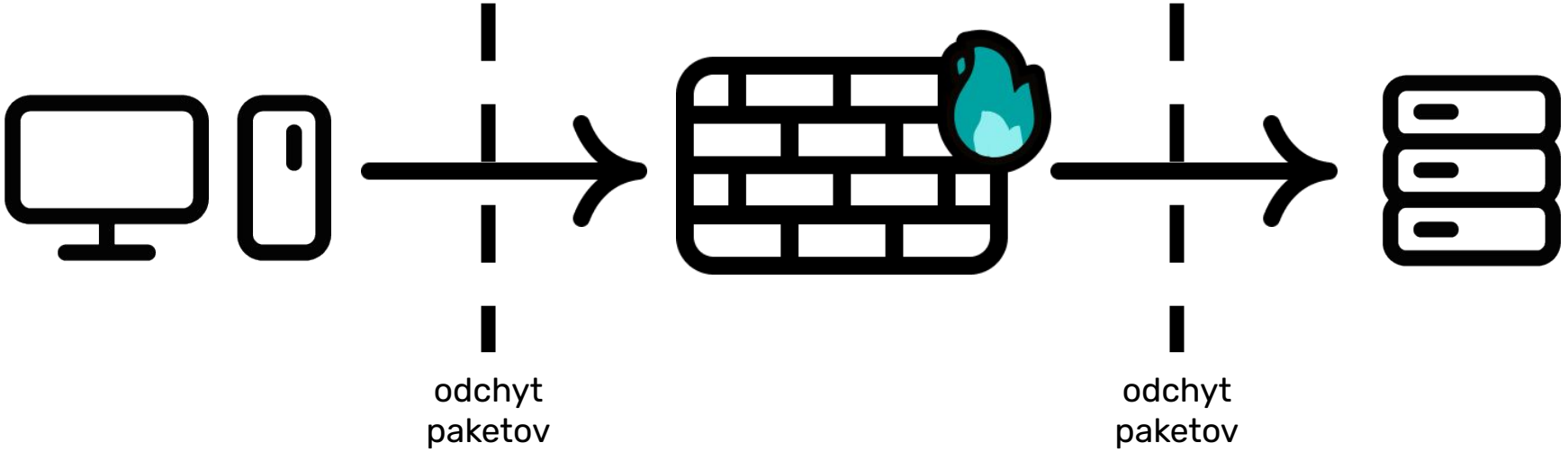
ZHRNUTIE

- vytvorili sme funkčnú implementáciu schopnú:
  - analyzovať vybrané aplikačné protokoly
  - brániť útokom
  - vymáhať bezpečnostnú politiku
- samotný vývoj a implementáciu sme popísali v texte práce
- otestovali sme funkčnosť a výkonové parametre implementácie

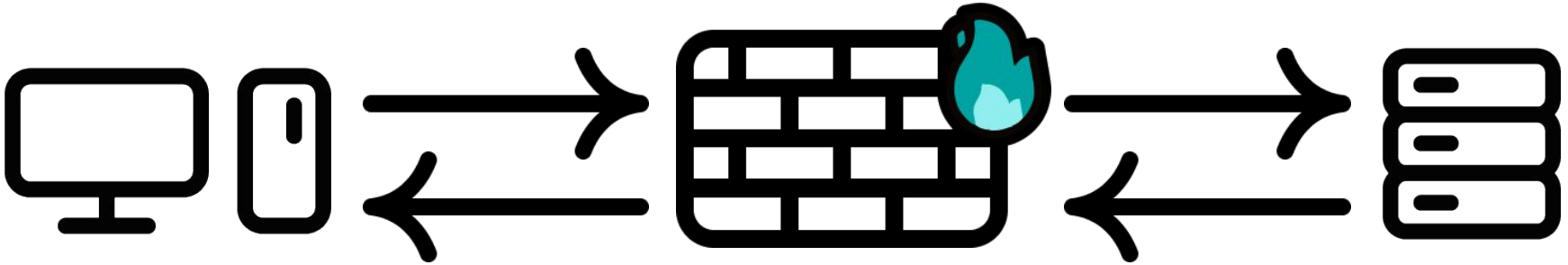
ĎAKUJEM ZA POZORNOSŤ

DISKUSIA

TESTOVACIE PROSTREDIE



TESTOVACIE PROSTREDIE



LIMIT NA DĹŽKU URI – MAX 20 ZNAKOV

URI: /

```
GET / HTTP/1.1
80 → 51592 [ACK] Seq=1 Ack=130 Win=31872 Len=0 TSval=3254217376
HTTP/1.1 200 OK  (text/html)
51592 → 80 [ACK] Seq=130 Ack=585 Win=31872 Len=0 TSval=90108862
```

URI: /a_very_long_request_uri.html

```
GET /a_very_long_request_uri.html HTTP/1.1
[TCP Retransmission] 51598 → 80 [PSH, ACK] Seq=1 Ack=1 Win=32128 Len=157
[TCP Retransmission] 51598 → 80 [PSH, ACK] Seq=1 Ack=1 Win=32128 Len=157
[TCP Retransmission] 51598 → 80 [PSH, ACK] Seq=1 Ack=1 Win=32128 Len=157
```