

# Implementácia distribuovaného firewallu založeného na OpenFlow

BEŇO, HARVAN

# Obsah prezentácie

- Objasnenie témy
- Experiment
- Naša nadstavba na článok

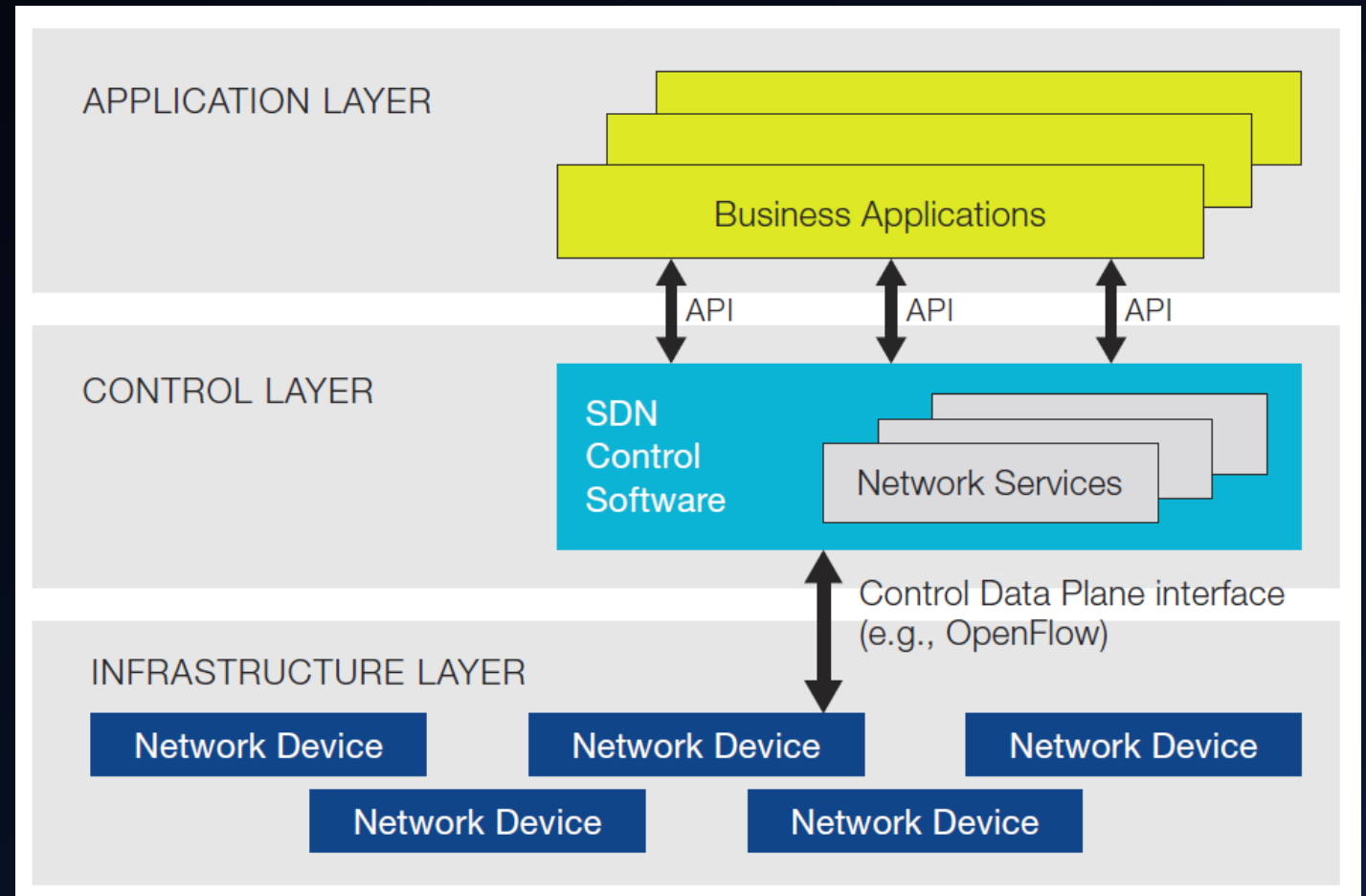


# Objasnenie témy

ARCHITEKTÚRA SDN

# Architektúra SDN

- Aplikačná vrstva – firewall
- Kontrolná vrstva – POX kontrolér
- Sieťová vrstva – jednotlivé prepínače

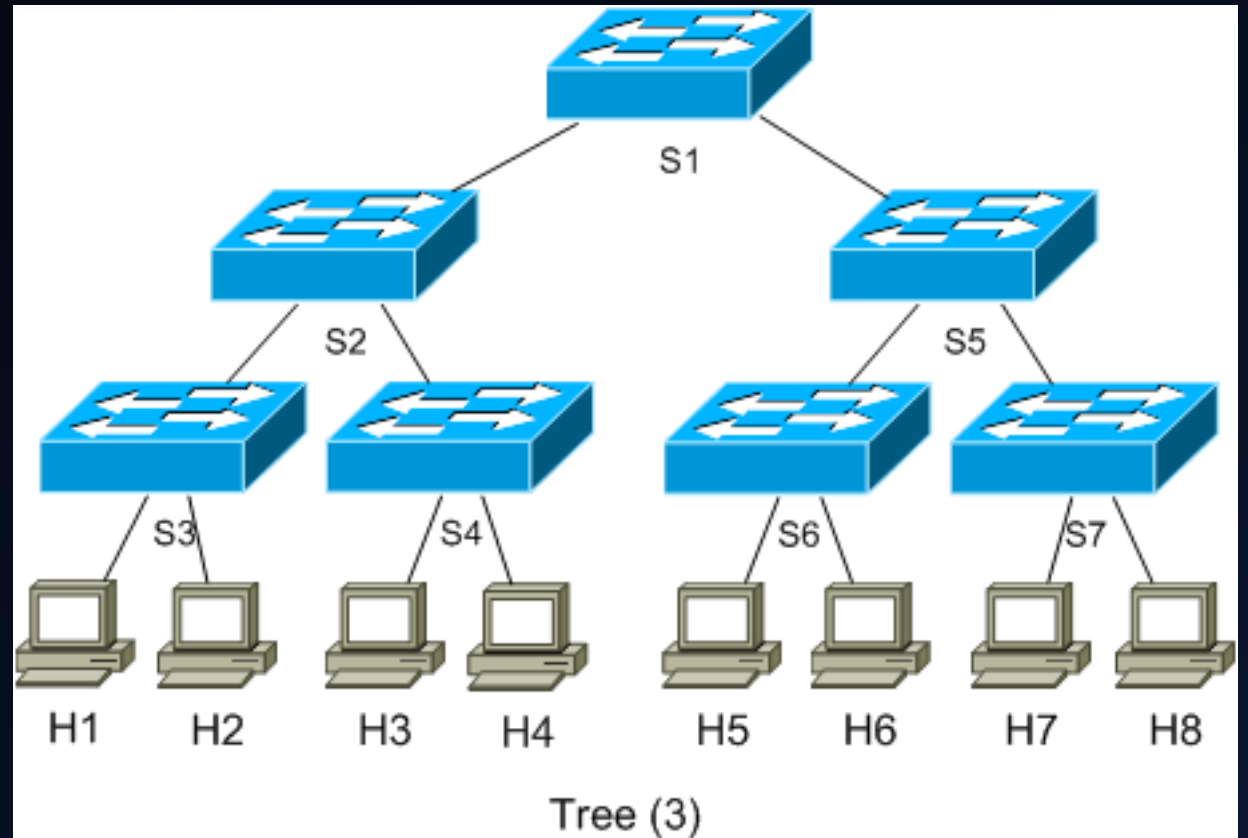


# Experiment

TESTOVANIE FUNKČNOSTI FIREWALLU  
TOPOLÓGIA SIETE

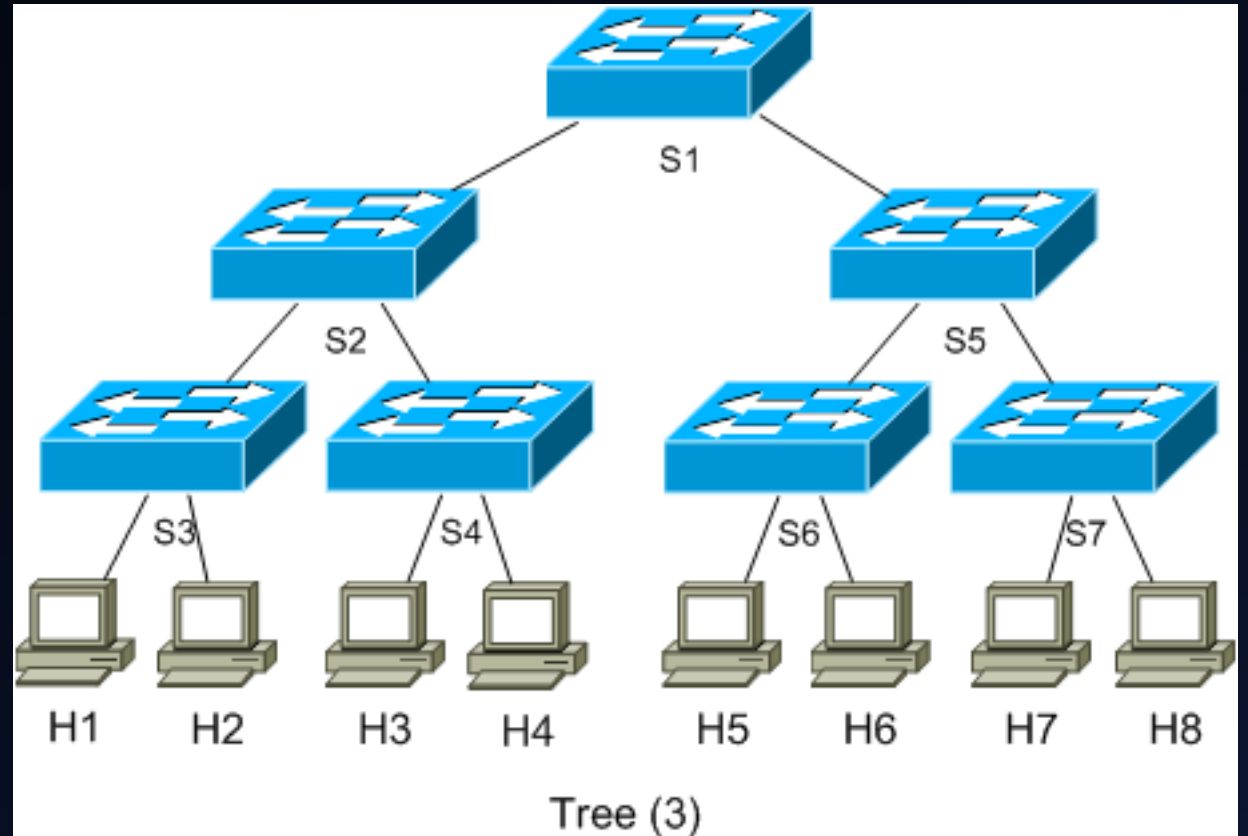
# Topológia siete

- Stromová topológia
- 7 prepínačov
- 8 hostov
  - IP: 10.0.0.1-8



# Testované scenáre

1. H1 nepingne H2
2. H1 nepigne H7
3. H1 nepristúpi na web server na H4
4. H7 nepristúpi na UDP port 53 na H8



# Tabuľka pravidiel blokovania komunikácie

Prepínač	Zdrojová IP	Cieľová IP	Protokol	Port
S3	10.0.0.1	10.0.0.2	1(ICMP)	-
S1	10.0.0.1	10.0.0.7	1(ICMP)	-
S2	10.0.0.1	10.0.0.4	6(TCP)	80
S7	10.0.0.7	10.0.0.8	17(UDP)	53



# Nastavenie pravidiel

- ID prepínača
- A, D, S – pridanie, vymazanie, vyhľadanie pravidiel
- Zdrojová a cieľová IP
- Protokol
  - Port

```
Enter the DPID of switch in which you want to insert, delete or show rules: 3
Enter 'A' for adding, 'D' for deleting, 'S' for showing the rules: 'A'
Enter any of the following matching fields
Source IP, Destination IP, Network Protocol, Destination port(UDP or TCP)
Source IP Address(Press Enter for None): 10.0.0.1
Destination IP address(Press Enter for None): 10.0.0.2
Enter Network Protocol(1 for ICMP, 6 for TCP, 17 for UDP): 1
('adding Rule:', (2048, IPAddr('10.0.0.1'), IPAddr('10.0.0.2'), 1))
Enter the DPID of switch in which you want to insert, delete or show rules: 1
Enter 'A' for adding, 'D' for deleting, 'S' for showing the rules: 'A'
Enter any of the following matching fields
Source IP, Destination IP, Network Protocol, Destination port(UDP or TCP)
Source IP Address(Press Enter for None): 10.0.0.1
Destination IP address(Press Enter for None): 10.0.0.7
Enter Network Protocol(1 for ICMP, 6 for TCP, 17 for UDP): 1
('adding Rule:', (2048, IPAddr('10.0.0.1'), IPAddr('10.0.0.7'), 1))

Enter the DPID of switch in which you want to insert, delete or show rules: 2
Enter 'A' for adding, 'D' for deleting, 'S' for showing the rules: 'A'
Enter any of the following matching fields
Source IP, Destination IP, Network Protocol, Destination port(UDP or TCP)
Source IP Address(Press Enter for None): 10.0.0.1
Destination IP address(Press Enter for None): 10.0.0.4
Enter Network Protocol(1 for ICMP, 6 for TCP, 17 for UDP): 6
Enter TCP or UDP destination port: 80
('adding Rule:', (2048, IPAddr('10.0.0.1'), IPAddr('10.0.0.4'), 6, 80))

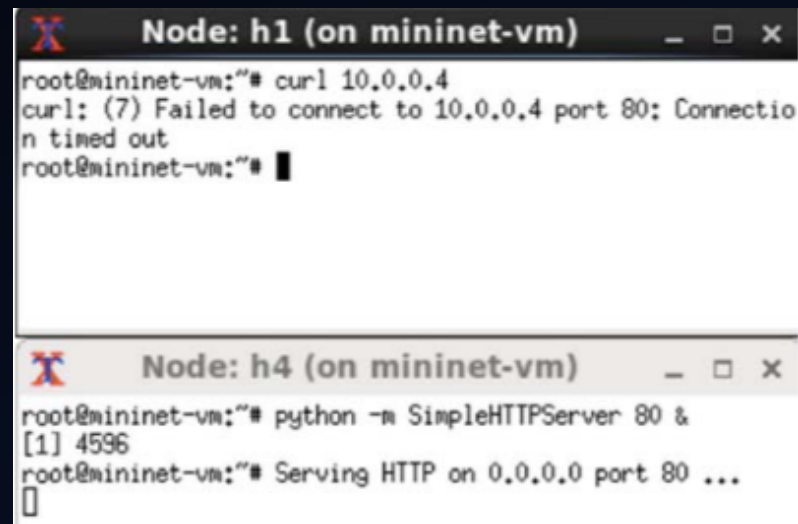
Enter the DPID of switch in which you want to insert, delete or show rules: 7
Enter 'A' for adding, 'D' for deleting, 'S' for showing the rules: 'A'
Enter any of the following matching fields
Source IP, Destination IP, Network Protocol, Destination port(UDP or TCP)
Source IP Address(Press Enter for None): 10.0.0.7
Destination IP address(Press Enter for None): 10.0.0.8
Enter Network Protocol(1 for ICMP, 6 for TCP, 17 for UDP): 17
Enter TCP or UDP destination port: 53
('adding Rule:', (2048, IPAddr('10.0.0.7'), IPAddr('10.0.0.8'), 17, 53))
```

# Testovanie a výsledky

## TESTOVACÍ SCENÁR 1,2

```
mininet> pingall
*** Ping: testing ping reachability
h1 -> X h3 h4 h5 h6 X h8
h2 -> X h3 h4 h5 h6 h7 h8
h3 -> h1 h2 h4 h5 h6 h7 h8
h4 -> h1 h2 h3 h5 h6 h7 h8
h5 -> h1 h2 h3 h4 h6 h7 h8
h6 -> h1 h2 h3 h4 h5 h7 h8
h7 -> X h2 h3 h4 h5 h6 h8
h8 -> h1 h2 h3 h4 h5 h6 h7
*** Results: 7% dropped (52/56 received)
```

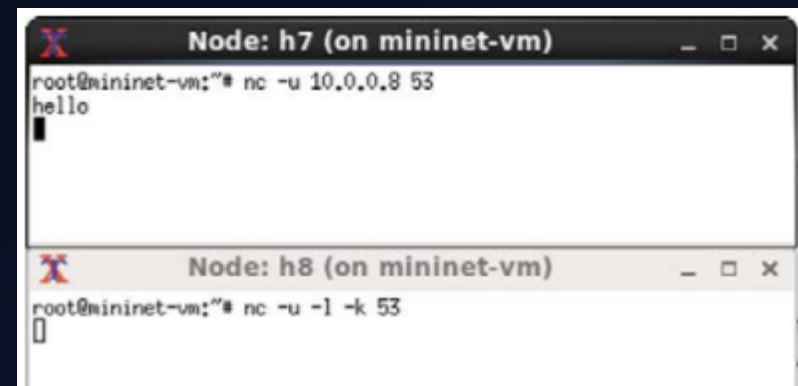
## TESTOVACÍ SCENÁR 3



```
Node: h1 (on mininet-vm)
root@mininet-vm:~# curl 10.0.0.4
curl: (7) Failed to connect to 10.0.0.4 port 80: Connection timed out
root@mininet-vm:~#

Node: h4 (on mininet-vm)
root@mininet-vm:~# python -m SimpleHTTPServer 80 &
[1] 4596
root@mininet-vm:~# Serving HTTP on 0.0.0.0 port 80 ...
```

## TESTOVACÍ SCENÁR 4



```
Node: h7 (on mininet-vm)
root@mininet-vm:~# nc -u 10.0.0.8 53
hello

Node: h8 (on mininet-vm)
root@mininet-vm:~# nc -u -l -k 53
```

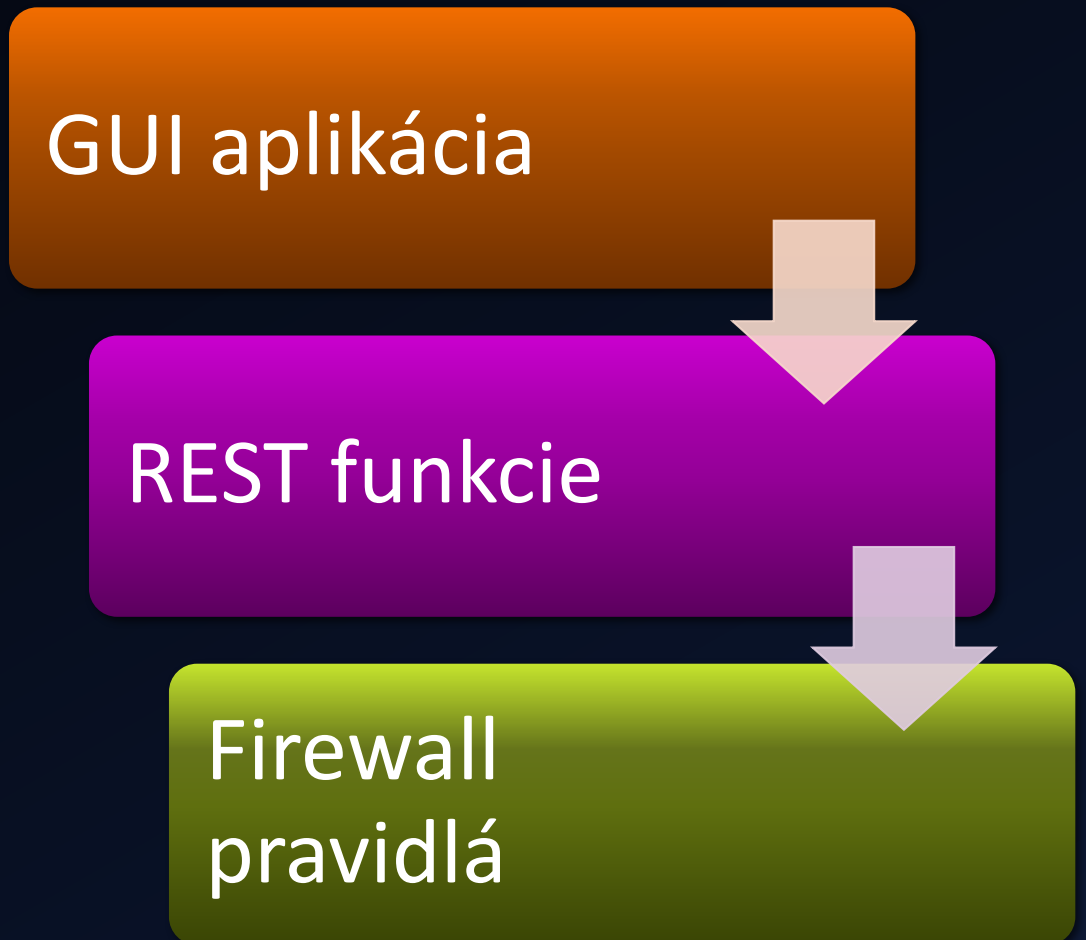


# Naša práca

## GRAFICKÉ ROZHRAŇIE

# Použitý firewall

- RYU rest firewall
- Black list vs. White list
- Npm
- jQuery – ajax



# Aktuálny stav prototypu

The screenshot displays a web application prototype in a browser window. The browser's address bar shows '0.0.0.0'. The application has a header with the 'Admin' title and a hamburger menu icon. A sidebar on the left contains a menu with four items: 'Dashboard' (home icon), 'Rules' (list icon), 'Logs' (document icon), and 'Network' (globe icon). The main content area is titled 'IP address' and contains a form with the label 'IP address (e.g.: 192.168.56.101:8080):'. Below the label is a text input field with the placeholder 'IP address'. A blue 'Put' button is positioned below the input field. The footer of the application contains the text 'Copyright © 2017 Designed by Colorlib. All rights reserved.'

Admin

- Dashboard
- Rules
- Logs
- Network

IP address

IP address (e.g.: 192.168.56.101:8080):

Put

Copyright © 2017 Designed by Colorlib. All rights reserved.

# Aktuálny stav prototypu

The screenshot shows a web application interface for managing a firewall. The browser address bar displays '0.0.0.0'. The application has a sidebar with navigation links: Admin, Dashboard, Rules, Logs, and Network. The main content area is titled 'Firewall status:' and displays a table of firewall rules. All rules are currently disabled. The table has three columns: ID, Enabled, and an action button. The IP address '192.168.56.101:8080' is shown in the top right corner. The footer contains copyright information: 'Copyright © 2017 Designed by Colorlib. All rights reserved.'

ID	Enabled	Action
0000000000000001	disabled	enable
0000000000000002	disabled	enable
0000000000000003	disabled	enable
0000000000000004	disabled	enable
0000000000000005	disabled	enable
0000000000000006	disabled	enable
0000000000000007	disabled	enable