



*Elektrotehnički fakultet u Beogradu
Katedra za računarsku tehniku i informatiku*

Zaštita računarskih sistema i mreža

- Peta laboratorijska vežba -

Podешavanje laboratorijskog okruženja.

Programom *Putty* povezati se *SSH* protokolom na sve tri virtuelne mašine.

1. Na VM2 proveriti da li je uključeno rutiranje komandom:

```
cat /proc/sys/net/ipv4/ip_forward
```

Ako se dobije 0, znači da rutiranje nije uključeno i treba ga uključiti komandom:

```
sudo sysctl -w net.ipv4.ip_forward=1
```

Proveriti ponovo da li je rutiranje uključeno.

2. Podići interfejsе i uspostaviti rutiranje između VM1 i VM3 kroz VM2:

- VM1

```
sudo ip link set eth1 up  
sudo ip addr add 10.12.x.1/24 dev eth1  
sudo ip route add 10.23.x.0/24 via 10.12.x.2
```

- VM2

```
sudo ip link set eth1 up  
sudo ip addr add 10.12.x.2/24 dev eth1  
sudo ip link set eth2 up  
sudo ip addr add 10.23.x.2/24 dev eth2
```

- VM3

```
sudo ip link set eth2 up  
sudo ip addr add 10.23.x.3/24 dev eth2  
sudo ip route add 10.12.x.0/24 via 10.23.x.2
```

3. Proveriti da li paketi prolaze između VM1 i VM3. Na VM3 izvršiti komandu:

```
ping 10.12.x.1  
tracert 10.12.x.1
```

Očekivani izlaz:

```
tracert to 10.12.x.1 (10.12.x.1), 30 hops max, 60 byte packets  
 0 10.23.x.2 (10.23.x.2) 0.274 ms 0.207 ms 0.174 ms  
 1 10.12.x.2 (10.12.x.2) 0.415 ms 0.401 ms 0.371 ms
```

4. Podizanje servisa na VM3:

- Instalirati FTP server pomoću komande:

```
sudo apt install vsftpd  
sudo systemctl restart vsftpd.service  
sudo python3 -m /home/student/Documents/web/http.server 80  
(ili cd /home/student/Documents/web pa onda sudo python3 -m http.server 80)  
(podrazumeva se da je na tom mestu web server iz prethodne lab. vežbe)
```

- Proveriti na VM1 da li su dostupni *ftp*, *ssh* i *web* servisi:

```
ftp 10.23.x.3 (izlaz pomoću quit)  
ssh 10.23.x.3  
curl 10.23.x.3
```

Uspostavljanje paketskog filtera.

Primer 1.

Na VM2 proveriti koja su postavljena pravila komandom:

```
sudo iptables -L
```

I za dolazeće i za odlazeće i za pakete koji se rutiraju je *policy accept*

Postavljanje politike *DROP* za rutiranje (*FORWARD*) kojim se svi paketi filtriraju:

```
sudo iptables --policy FORWARD DROP
```

Proveriti ponovo sadržaj tabele filtriranja:

```
sudo iptables -L
```

Probati ponovo sve servise na VM1 kao u drugom *bullet*-u tačke 4.

Vratiti *FORWARD* polisu na *ACCEPT*:

```
sudo iptables --policy FORWARD ACCEPT
```

Postaviti *FORWARD* filter za *ssh*

```
sudo iptables -A FORWARD -i eth1 -p tcp --dport 22 -d 10.23.x.3 -j DROP
```

Proveriti ponovo sadržaj tabele filtriranja:

```
sudo iptables -L
```

Probati ponovo sve servise.

Postaviti *FORWARD* filter za *web*

```
sudo iptables -A FORWARD -i eth1 -p tcp --dport 80 -d 10.23.x.3 -j DROP
```

Proveriti ponovo sadržaj tabele filtriranja:

```
sudo iptables -L
```

Probati ponovo sve servise.

Postaviti *FORWARD* filter za *ftp*

```
sudo iptables -A FORWARD -i eth1 -p tcp --dport 21 -d 10.23.x.3 -j DROP
```

Proveriti ponovo sadržaj tabele filtriranja:

```
sudo iptables -L
```

Probati ponovo sve servise.

Vratiti tabele filtriranja na početni status:

```
sudo iptables -F
```

```
sudo iptables -X
```

Primer 2.

Postaviti sledeći filter:

```
sudo iptables -A FORWARD -i eth1 -p tcp --dport 22 -d 10.23.x.3 -j ACCEPT
```

```
sudo iptables -A FORWARD -i eth1 -p tcp -d 10.23.x.3 -j DROP
```

Probati ponovo sve servise.

Vratiti tabele filtriranja na početni status:

```
sudo iptables -F
```

```
sudo iptables -X
```

Postaviti sledeći filter:

```
sudo iptables -A FORWARD -i eth1 -p tcp -d 10.23.x.3 -j DROP
sudo iptables -A FORWARD -i eth1 -p tcp --dport 22 -d 10.23.x.3 -j ACCEPT
```

Probati ponovo sve servise.

Koja je razlika između slučaja 1 i 2?

Zašto postoji ova razlika?

Vratiti tabele filtriranja na početni status:

```
sudo iptables -F
sudo iptables -X
```

Primer 3.

Na VM2 postaviti sledeće filtere:

```
sudo iptables -A FORWARD -i eth1 -p tcp --dport 22 -d 10.23.x.3 -j DROP
sudo iptables -A FORWARD -i eth1 -p tcp -d 10.23.x.3 -j ACCEPT
```

Na VM3 postaviti sledeći filter:

```
sudo iptables -A INPUT -i eth2 -p tcp --dport 80 -d 10.23.x.3 -j DROP
```

Probati ponovo sve servise.

Koji uređaj je blokirao *web*, a koji *ssh* pakete?

Vratiti tabele filtriranja na početni status:

```
sudo iptables -F
sudo iptables -X
```

Primer 4.

Na VM2 postaviti sledeće filtere:

```
sudo iptables -A FORWARD -i eth2 -p tcp --sport 22 -s 10.23.x.3 -j DROP
sudo iptables -A FORWARD -i eth2 -p tcp -s 10.23.x.3 -j ACCEPT
```

Na VM3 otvoriti još jedan prozor i pokrenuti:

```
sudo tcpdump -i eth2 kojim se snimaju svi paketi koji prolaze kroz eth2 interfejs
```

Probati ponovo sve servise. Nakon toga prekinuti *tcpdump*.

Da li se na VM3 registruju paketi kojima VM1?

Zašto ne radi *ssh* sesija?

Koji paketi su filtrirani i gde?

Vratiti tabele filtriranja na početni status:

```
sudo iptables -F
sudo iptables -X
```

Primer 5.

Na VM2 postaviti sledeće filtere:

```
sudo iptables -A FORWARD -i eth1 -p ip -d 10.23.x.3 -j DROP
sudo iptables -A FORWARD -i eth1 -p tcp -d 10.23.x.3 -j ACCEPT
```

Probati ponovo sve servise i ping ka 10.23.x.3.

Zašto paketi ne prolaze?

Šta filtrira prvi, a šta filtrira drugi red tabele filtriranja?

Vratiti tabele filtriranja na početni status:

```
sudo iptables -F
```

```
sudo iptables -X
```

Primer 6.

Na VM 2 postaviti sledeće filtere:

```
sudo iptables -A FORWARD -i eth1 -p ip -d 10.23.x.0/24 -j DROP
```

```
sudo iptables -A FORWARD -i eth1 -p ip -d 10.23.x.3 -j ACCEPT
```

Probati ponovo sve servise i ping ka 10.23.x.3

Vratiti tabele filtriranja na početni status:

```
sudo iptables -F
```

```
sudo iptables -X
```

Sada postaviti filtere:

```
sudo iptables -A FORWARD -i eth1 -p ip -d 10.23.x.3 -j ACCEPT
```

```
sudo iptables -A FORWARD -i eth1 -p ip -d 10.23.x.0/24 -j DROP
```

Probati ponovo sve servise i ping ka 10.23.x.3

Koja je razlika između prvog i drugog slučaja?

Firewall

Podešavanje Firewall-a.

Na VM1 podići interfejs prema Firewallu, podesiti ip adresu i konfigurisati rute:

```
sudo ip link set dev eth3 up
sudo ip addr add 192.168.1.100/24 dev eth3
sudo ip route add 10.24.x.0/24 via 192.168.1.1
sudo ip route add 10.34.x.0/24 via 192.168.1.1
```

Na VM2 podići interfejs prema Firewallu, podesiti ip adresu i konfigurisati rute:

```
sudo ip link set dev eth3 up
sudo ip addr add 10.24.x.2/24 dev eth3
sudo ip route add 192.168.1.0/24 via 10.24.x.4
sudo ip route add 10.34.x.0/24 via 10.24.x.4
```

Na VM3 podići interfejs prema Firewallu, podesiti ip adresu i konfigurisati rute:

```
sudo ip link set dev eth3 up
sudo ip addr add 10.34.x.3/24 dev eth3
sudo ip route add 192.168.1.0/24 via 10.34.x.4
sudo ip route add 10.24.x.0/24 via 10.34.x.4
```

Preko VNC veze ka VM1 povezati se iz *Firefox browser-a* na *Firewall*:

Adresa firewalla: 192.168.1.1

Username: admin

Pasword: pfsense

Kliknuti na tab sa interfejsima i dodati još jedan interfejs (OPT2):

The screenshot shows the pfSense web interface. The browser address bar displays `https://192.168.1.1/interfaces_assign.php`. The navigation menu includes 'System', 'Interfaces', 'Firewall', 'Services', 'VPN', 'Status', 'Diagnostics', and 'Help'. A warning message is present: 'WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager.' The main content area is titled 'Interfaces / Interface Assignments'. It features a tabbed interface with 'Interface Assignments' selected. The table below shows the following data:

Interface	Network port
WAN	vmx2 (00:50:56:ac:4d:14)
LAN	vmx1 (00:50:56:ac:3d:7e)
OPT2	vmx3 (00:50:56:ac:a6:1d)

Below the table, the 'Available network ports' section shows 'vmx0 (00:50:56:ac:66:ff)' with an 'Add' button. A 'Save' button is located at the bottom left of the interface.

LAN (vmx1) interfejs je povezan sa VM1, WAN (vmx2) sa VM2 i OPT2 (vmx3) sa VM3
LAN interfejs je konfigurisan i ima adresu 192.168.1.1.

Konfigurisati WAN interfejs klikom na WAN. Postaviti statičku IP adresu 10.24.x.4/24

Enable	<input checked="" type="checkbox"/> Enable interface
Description	<input type="text" value="WAN"/> Enter a description (name) for the interface here.
IPv4 Configuration Type	Static IPv4
IPv6 Configuration Type	DHCP6
MAC Address	<input type="text" value="xx:xx:xx:xx:xx:xx"/> This field can be used to modify ("spoof") the MAC address of this interface. Enter a MAC address in the following format: xx:xx:xx:xx:xx:xx or leave blank.
MTU	<input type="text"/> If this field is blank, the adapter's default MTU will be used. This is typically 1500 bytes but can vary in some circumstances.
MSS	<input type="text"/> If a value is entered in this field, then MSS clamping for TCP connections to the value entered above minus 40 (TCP/IP header size) will be used.
Speed and Duplex	Default (no preference, typically autoselect) Explicitly set speed and duplex mode for this interface. WARNING: MUST be set to autoselect (automatically negotiate speed) unless the port this interface connects to has its speed and duplex mode set to autoselect.

Static IPv4 Configuration

IPv4 Address	<input type="text" value="10.24.198.4"/>	/	24
--------------	--	---	----

Odselektovati oba kriterijuma u delu *reserved networks*.

Reserved Networks

Block private networks and loopback addresses	<input type="checkbox"/> Blocks traffic from IP addresses that are reserved for private networks per RFC 1918 (10/8, 172.16/12, 192.168/16) and unique local addresses per RFC 4193 (fc00::/7) as well as loopback addresses (127/8). This option should generally be turned on, unless this network interface resides in such a private address space, too.
Block bogon networks	<input type="checkbox"/> Blocks traffic from reserved IP addresses (but not RFC 1918) or not yet assigned by IANA. Bogons are prefixes that should never appear in the Internet routing table, and so should not appear as the source address in any packets received. Note: The update frequency can be changed under System > Advanced, Firewall & NAT settings.

Snimiti konfiguraciju (*Save* na dnu strane)

Konfigurisati OPT2 (vmx3) interfejs klikom na OPT2. Postaviti statičku adresu 10.34.x.4

Enable	<input checked="" type="checkbox"/> Enable interface
Description	<input type="text" value="OPT2"/> Enter a description (name) for the interface here.
IPv4 Configuration Type	Static IPv4
IPv6 Configuration Type	None
MAC Address	<input type="text" value="xx:xx:xx:xx:xx:xx"/> This field can be used to modify ("spoof") the MAC address of this interface. Enter a MAC address in the following format: xx:xx:xx:xx:xx:xx or leave blank.
MTU	<input type="text"/> If this field is blank, the adapter's default MTU will be used. This is typically 1500 bytes but can vary in some circumstances.
MSS	<input type="text"/> If a value is entered in this field, then MSS clamping for TCP connections to the value entered above minus 40 (TCP/IP header size) will be used.
Speed and Duplex	Default (no preference, typically autoselect) Explicitly set speed and duplex mode for this interface. WARNING: MUST be set to autoselect (automatically negotiate speed) unless the port this interface connects to has its speed and duplex mode set to autoselect.

Static IPv4 Configuration

IPv4 Address	<input type="text" value="10.34.198.4"/>	/	24
--------------	--	---	----

Snimiti konfiguraciju (*Save* na dnu strane)

Na kraju konfiguracije uraditi Apply changes (zeleno dugme u gornjem desnom uglu).

Vežba 1 – Podešavanje jednostavnih pravila.

Proveriti da li je sve dobro povezano.

Sa računara VM1 uraditi ping 10.24.x.2

Sa računara VM1 uraditi ping 10.34.x.3

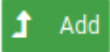
Probati sa VM2 i VM3 ping na 192.168.1.100. Da li radi?

Kliknuti na *Tab Firewall/Rules* i pogledati predefinisana pravila za LAN, WAN i OPT2. Šta piše za pravila za WAN i OPT2? Zašto ne radi ping sa VM2 I VM3?

Probati sa VM1 *ssh*, *ftp* i *web* servis prema 10.34.x.3

Da li radi?

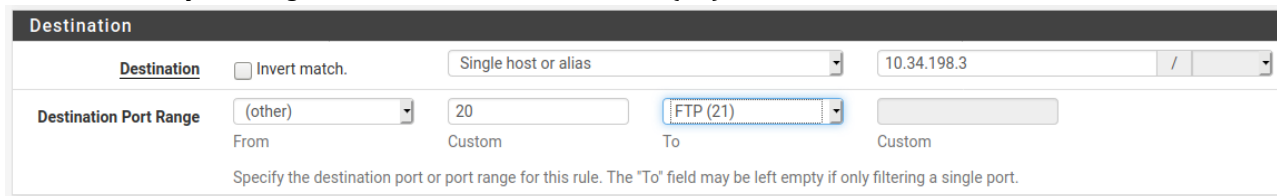
Zašto prolaze paketi od VM1 ka VM3?

Otići na tab za podešavanje LAN pravila I kliknuti na dugme  kojim se dodaje pravilo koje se smešta na vrh liste.

U okviru dela *Edit Firewall Rule* treba da stoji akcija *Pass*.

U okviru dela *destination* postaviti *Destination – Single host or alias* i adresu 10.34.x.3

Za *destination port range* odabrati *Custom* 20 do FTP (21):



Snimiti pravilo.

Otvoriti još jedno pravilo na isti način kao prethodno.

Podesiti akciju *Block*

U okviru dela *destination* postaviti *Destination – Single host or alias* i adresu 10.34.x.3

Za *destination port range* upisati u polje *Custom* 22

Snimiti pravilo. Nakon povratka na stranu sa listom pravila kliknuti na *Apply Changes*.

Na VM1 probati sve servise.

Vežba 2 – Razlika između paket filtera i stateful firewall-a.

Postaviti sledeći filter:

```
sudo iptables -A FORWARD -i eth2 -p tcp --sport 22 -s 10.23.x.3 -j DROP
```

Na VM1 probati *ssh* konekciju prema VM3:

```
ssh student@10.23.x.3
```

```
ssh student@10.34.x.3
```

Da li prolaze konekcije? Zašto?

Na VM1 probati *ftp* konekciju prema VM3:

```
ftp 10.23.x.3
```

```
ftp 10.34.x.3
```

Da li prolaze konekcije? Zašto?

Na VM1 pokrenuti snimanje paketa:

```
sudo tcpdump -i eth1
```

Na VM3 pokrenuti komandu:

```
sudo hping3 -c 3 -p 12345 -s 22 10.12.x.1
```

Da li su paketi prošli?

Na VM3 pokrenuti komandu:

```
sudo hping3 -c 3 -p 12345 -s 21 10.12.x.1
```

Da li su paketi prošli?

Prekinuti *tcpdump* na VM1.

Na VM1 pokrenuti snimanje paketa:

```
sudo tcpdump -i eth3
```

Na VM3 pokrenuti komandu:

```
sudo hping3 -c 3 -p 12345 -s 22 192.168.1.100
```

Da li su paketi prošli? Zašto?

Na VM3 pokrenuti komandu:

```
sudo hping3 -c 3 -p 12345 -s 21 192.168.1.100
```

Da li su paketi prošli? Zašto?

Otvoriti još jedan prozor na VM1.

Pokrenuti FTP sesiju:

```
ftp 10.34.x.3
```

Ulogovati se u sesiju i ostaviti je aktivnu.

Na VM3 uraditi

```
netstat -at
```

Pronaći u ispisu komande red u kojem je ova *ftp* sesija sa VM1:

```
tcp6          0          0 ibLab-98-VM3:ftp      192.168.1.100:39544      ESTABLISHED
```

Zabeležiti port koji se koristi u toj sesiji (u ovom primeru **39544**).

Pokrenuti komandu (koristeći zabeleženi broj porta):

```
sudo hping3 -c 1000 -i u5000 -p 39544 -s 21 -k -A -w 502 192.168.1.100
```

Da li se na VM1 vide paketi¹? Da li su paketi prošli kroz *firewall*?

¹ Neće proći svi paketi jer firewall prati stanje sesije (uključujući i sekvencijalne brojeve u TCP sesiji). Sa ovom konfiguracijom komanda *hping3* daje slučajne vrednosti ovih brojeva, te će proći samo neki paketi. Probati više puta, makar neki paketi će morati da prođu.

Prekinuti FTP sesiju na VM1. U *pfsense web* interfejsu otići na *Diagnostics/States* i pregledati dinamička stanja filtera u kojima se vidi za koje sesije je *firewall* otvorio prolaz paketima. Ovo izgleda ovako:

Diagnostics / States / States

States

Reset States

State Filter

Interface

all

Filter expression

Simple filter such as 192.168, v6, icmp or ESTABLISHED

Filter

States

Interface	Protocol	Source (Original Source) -> Destination (Original Destination)	State	Packets	Bytes
LAN	tcp	192.168.1.100:51464 -> 192.168.1.1:443	ESTABLISHED:ESTABLISHED	597 / 1.148 K	56 KiB / 1.13 MiB
LAN	tcp	192.168.1.100:39544 -> 10.34.198.3:21	ESTABLISHED:ESTABLISHED	19 / 18	1 KiB / 896 B
OPT2	tcp	192.168.1.100:39544 -> 10.34.198.3:21	ESTABLISHED:ESTABLISHED	19 / 18	1 KiB / 896 B

Pronaći stanje za ovu ftp sesiju i obrisati ga (simbol kante na kraju reda).

Probati ponovo:

```
sudo hping3 -c 1000 -i u5000 -p 39544 -s 21 -k -A -w 502 192.168.1.100
```

Da li se na VM1 vide neki paketi koji dolaze od VM3? Zašto?

Koja je razlika između klasičnog filtriranja paketa i *stateful firewall*-a? Razmisliti, u čemu je prednost *stateful firewall*-a u odnosu na obični paket filter.