



НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ імені Ігоря Сікорського»
ФАКУЛЬТЕТ ПРИКЛАДНОЇ МАТЕМАТИКИ

Лабораторна робота №7

з дисципліни «Системне програмне забезпечення»

«Конфігурування різноманітних міжмережених екранів»

Виконав студент IV курсу

групи: КВ-11

ПІБ: Терентьєв Іван Дмитрович

Перевірив: _____

Київ 2024

```

eth0      Link encap:Ethernet  HWaddr 00:0C:29:43:9C:A6
          inet addr:192.168.0.15  Bcast:192.168.0.255  Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:675 errors:0 dropped:0 overruns:0 frame:0
          TX packets:568 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:143092 (139.7 KB)  TX bytes:258136 (252.0 KB)
          Interrupt:9 Base address:0x1080

eth1      Link encap:Ethernet  HWaddr 00:0C:29:43:9C:B0
          inet addr:10.10.1.1  Bcast:10.10.1.255  Mask:255.255.255.0
          UP BROADCAST RUNNING  MTU:1500  Metric:1
          RX packets:60 errors:0 dropped:0 overruns:0 frame:0
          TX packets:25 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:14494 (14.1 KB)  TX bytes:1720 (1.6 KB)
          Interrupt:10 Base address:0x1400

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:4 errors:0 dropped:0 overruns:0 frame:0
          TX packets:4 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          :

```

Рис. 1 – Налаштування IP-адрес інтерфейсів Green (192.168.0.15) та Red (10.10.1.1) на IPCor.

```

root@ipcop:~ # ping 192.168.0.15
PING 192.168.0.15 (192.168.0.15): 56 data bytes
64 bytes from 192.168.0.15: icmp_seq=0 ttl=64 time=0.073 ms
64 bytes from 192.168.0.15: icmp_seq=1 ttl=64 time=0.048 ms
--- 192.168.0.15 ping statistics ---
2 packets transmitted, 2 packets received, 0% packet loss
round-trip min/avg/max/stddev = 0.048/0.060/0.073/0.000 ms
root@ipcop:~ # ping 10.10.1.1
PING 10.10.1.1 (10.10.1.1): 56 data bytes
64 bytes from 10.10.1.1: icmp_seq=0 ttl=64 time=0.053 ms
64 bytes from 10.10.1.1: icmp_seq=1 ttl=64 time=0.105 ms
64 bytes from 10.10.1.1: icmp_seq=2 ttl=64 time=0.088 ms
--- 10.10.1.1 ping statistics ---
3 packets transmitted, 3 packets received, 0% packet loss
round-trip min/avg/max/stddev = 0.053/0.082/0.105/0.000 ms
root@ipcop:~ # _

```

Рис. 2 – Перевірка доступності Green та Red інтерфейсів IPCor за допомогою команди ping.

```

root@Host741:~ # ping 10.10.1.1
PING 10.10.1.1 (10.10.1.1): 56 data bytes
^C
--- 10.10.1.1 ping statistics ---
21 packets transmitted, 0 packets received, 100.0% packet loss
root@Host741:~ # ping 10.10.1.1
PING 10.10.1.1 (10.10.1.1): 56 data bytes
64 bytes from 10.10.1.1: icmp_seq=0 ttl=64 time=0.167 ms
64 bytes from 10.10.1.1: icmp_seq=1 ttl=64 time=0.277 ms
64 bytes from 10.10.1.1: icmp_seq=2 ttl=64 time=0.268 ms
^C
--- 10.10.1.1 ping statistics ---
3 packets transmitted, 3 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 0.167/0.237/0.277/0.050 ms
root@Host741:~ #

```

Рис. 3 – Перевірка пінгу Red інтерфейсу IPCor з іншого вузла (FreeBSD).

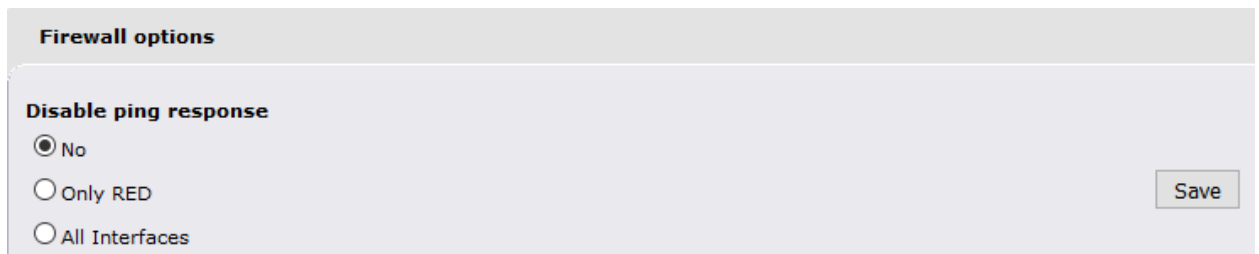


Рис. 4 – Налаштування правил у брандмауері IPCor для дозволу або блокування ICMP (ping).

```

root@Host741:~ # ipfw add 65534 allow all from any to any
65534 allow ip from any to any
root@Host741:~ # ipfw list
65534 allow ip from any to any
65535 deny ip from any to any
root@Host741:~ #

```

Рис. 5 – Додавання правила в ipfw на FreeBSD для дозволу всього трафіку.

```

root@Host741:~ # ipfw delete 65534
root@Host741:~ # ipfw list
65535 deny ip from any to any
root@Host741:~ #

```

Рис. 6 – Видалення правила в ipfw та перевірка списку правил після видалення.

```
root@Host741:~ # ipfw add 2207 allow tcp from any to 192.168.0.100
02207 allow tcp from any to 192.168.0.100
root@Host741:~ # ipfw add allow tcp from 192.168.0.100 to any
02307 allow tcp from 192.168.0.100 to any
root@Host741:~ # ipfw add 3308 allow udp from 192.168.0.10 53 to 192.168.0.100
03308 allow udp from 192.168.0.10 53 to 192.168.0.100
root@Host741:~ # ipfw add 3309 allow udp from 192.168.0.100 to 192.168.0.10 53
03309 allow udp from 192.168.0.100 to 192.168.0.10 dst-port 53
root@Host741:~ # ipfw list
02207 allow tcp from any to 192.168.0.100
02307 allow tcp from 192.168.0.100 to any
03308 allow udp from 192.168.0.10 53 to 192.168.0.100
03309 allow udp from 192.168.0.100 to 192.168.0.10 dst-port 53
65535 deny ip from any to any
root@Host741:~ # █
```

Рис. 7 – Додавання правил в ipfw для дозволу TCP-з'єднань між вузлами.

```
root@Host741:~ # ipfw flush
Are you sure? [yn] y

Flushed all rules.
root@Host741:~ # █
```

Рис. 8 – Видалення всіх правил в ipfw за допомогою команди ipfw flush.

Висновки

У ході виконання лабораторної роботи було проведено налаштування міжмережевого екрану IPСор та конфігурація мережевих правил на основі інструментів FreeBSD. Було виконано такі завдання:

- Проведено тестування доступності інтерфейсів за допомогою команди `ping`, що підтвердило коректність налаштувань.
- Виконано налаштування брандмауера IPСор для управління ICMP-запитами (пінгами) на різних інтерфейсах.
- Встановлено правила в `ipfw` на FreeBSD для дозволу або блокування TCP- та UDP-з'єднань між вузлами.
- Перевірено роботу мережі після застосування та видалення правил у брандмауері.

Практична частина дозволила закріпити знання з налаштування міжмережевих екранів та брандмауерів, а також отримати досвід роботи з такими інструментами, як `ipfw` на FreeBSD та налаштування правил в IPСор. Отримані результати демонструють важливість правильного управління мережевими правилами для забезпечення безпеки та доступності мереж.