

Санкт-Петербургский национальный исследовательский университет
Информационных технологий механики и оптики

Факультет информационных технологий и программирования

Лабораторная работа №5
По предмету Администрирование в информационных системах
«Firewall & NAT»

Исполнитель: Трофимов В.А.
Руководитель: Береснев А.Д.
Группа: 3511

Санкт-Петербург
2014

Цель работы

Сформировать понимание принципов работы NAT и firewall, а также начальные навыки в конфигурировании NAT.

Windows

Конфигурация

```
C:\WINDOWS\system32>netsh routing ip show rtmroutes
```

Префикс	Протокол	Прд	Мтр.	Шлюз	Вид	Интерфейс
0.0.0.0/0	NetMgmt	10	10	172.16.0.1	UM	Подключение по локальной сети
10.0.0.0/8	Local	1	10	10.0.0.1	UM	Подключение по локальной сети 2
10.0.0.1/32	Local	1	10	127.0.0.1	U	Замыкание на себя
10.255.255.255/32	Local	1	10	10.0.0.1	UM	Подключение по локальной сети 2
127.0.0.0/8	Local	1	1	127.0.0.1	U	Замыкание на себя
127.0.0.1/32	Local	1	1	127.0.0.1	U	Замыкание на себя
172.16.0.0/16	Local	1	10	172.16.0.10	UM	Подключение по локальной сети
172.16.0.10/32	Local	1	10	127.0.0.1	U	Замыкание на себя
172.16.255.255/32	Local	1	10	172.16.0.10	UM	Подключение по локальной сети
224.0.0.0/4	Local	1	10	10.0.0.1	UM	Подключение по локальной сети 2
224.0.0.0/4	Local	1	10	172.16.0.10	UM	Подключение по локальной сети
255.255.255.255/32	Local	1	1	10.0.0.1	UM	Подключение по локальной сети 2
255.255.255.255/32	Local	1	1	172.16.0.10	UM	Подключение по локальной сети

Скрипт настройки

```
sc config SharedAccess start= auto
netsh firewall set opmode ENABLE ENABLE
netsh firewall set logging c:\log.txt 8192 ENABLE
sc config TlntSvr start= demand
netsh firewall set icmpsetting 8 ENABLE
netsh firewall set portopening TCP 23 Telnet ENABLE ALL
net start telnet
```

Активные telnet сессии

```
C:\Documents and Settings\Admin>netstat -n -b
```

Активные подключения

Имя	Локальный адрес	Внешний адрес	Состояние	PID
TCP	10.0.0.10:23	172.16.0.1:1031	ESTABLISHED	2036
[tlntsvr.exe]				

Linux

Вывод iptables-save

```
# Generated by iptables-save v1.4.7 on Sat Dec 20 01:56:18 2014
*mangle
:PREROUTING ACCEPT [9:749]
:INPUT ACCEPT [1:229]
:FORWARD ACCEPT [8:520]
:OUTPUT ACCEPT [14:10864]
:POSTROUTING ACCEPT [0:0]
COMMIT
# Completed on Sat Dec 20 01:56:18 2014
# Generated by iptables-save v1.4.7 on Sat Dec 20 01:56:18 2014
*nat
:PREROUTING ACCEPT [321:35055]
:INPUT ACCEPT [85:12882]
:OUTPUT ACCEPT [479:29500]
:POSTROUTING ACCEPT [5:352]
```

```
-A PREROUTING -i eth2 -p tcp -m tcp --dport 2222 -j DNAT --to-destination 10.0.0.2:23
-A POSTROUTING -o eth2 -j MASQUERADE
COMMIT
# Completed on Sat Dec 20 01:56:18 2014
# Generated by iptables-save v1.4.7 on Sat Dec 20 01:56:18 2014
*filter
:INPUT DROP [1:229]
:FORWARD DROP [8:520]
:OUTPUT DROP [14:10864]
-A INPUT -m state --state NEW -m tcp -p tcp --dport 2222 -j ACCEPT
-A INPUT -i lo -j ACCEPT
-A INPUT -d 192.168.248.21/32 -i eth3 -p udp -m udp --sport 53 -j ACCEPT
-A INPUT -i eth3 -p icmp -m icmp --icmp-type 8 -j DROP
-A INPUT -d 194.85.160.50/32 -p tcp -m tcp --sport 143 -m state --state ESTABLISHED -j ACCEPT
-A INPUT -p tcp -m tcp --sport 110 -m state --state ESTABLISHED -j ACCEPT
-A INPUT -d 194.85.160.55/32 -p tcp -m tcp --sport 8080 -m state --state ESTABLISHED -j ACCEPT
-A INPUT -d 194.85.160.60/32 -p tcp -m tcp --sport 21 -m state --state ESTABLISHED -j ACCEPT
-A INPUT -d 10.10.11.173/32 -i eth2 -j DROP
-A INPUT -d 10.10.11.173/32 -i eth3 -j DROP
-A INPUT -d 83.0.0.0/16 -i eth2 -p tcp -m tcp --dport 22 -m state --state NEW,ESTABLISHED -j ACCEPT
-A FORWARD -d 192.168.1.152/32 -p tcp -m tcp --dport 22 -j ACCEPT
-A OUTPUT -p tcp -m tcp --dport 22 -j ACCEPT
-A OUTPUT -d 192.168.248.21/32 -o eth3 -p udp -m udp --dport 53 -j ACCEPT
-A OUTPUT -d 194.85.160.50/32 -p tcp -m tcp --dport 143 -m state --state NEW,ESTABLISHED -j ACCEPT
-A OUTPUT -p tcp -m tcp --dport 110 -m state --state NEW,ESTABLISHED -j ACCEPT
-A OUTPUT -d 194.85.160.55/32 -p tcp -m tcp --dport 8080 -m state --state NEW,ESTABLISHED -j ACCEPT
-A OUTPUT -d 194.85.160.60/32 -p tcp -m tcp --dport 21 -m state --state NEW,ESTABLISHED -j ACCEPT
-A OUTPUT -d 10.10.11.173/32 -j DROP
-A OUTPUT -d 83.0.0.0/16 -o eth2 -p tcp -m tcp --sport 22 -m state --state ESTABLISHED -j ACCEPT
COMMIT
# Completed on Sat Dec 20 01:56:18 2014
```