Лабораторна робота №8

з дисципліни «мережеві технології»

«Трансляція мережевих адрес (NAT)»

Виконав: студент групи ІП-73мп
Олександр Ковальчук

Контрольні запитання:

1. З якою метою застосовується технологія трансляції мережевих адрес?

   Технологія NAT використовується для забезпечення доступу до мережі внутрішніх вузлів, адреси яких знаходяться в приватному сегменті. Також дана технологія може використовуватися для приховання масштабів та структури внутрішньої мережі організації, а також структури та інтенсивності вхідного та вихідного трафіку.

2. Які обмеження накладаються на використання технології NAT?

   Усі запити та відповіді, які відносяться до одного сеансу, повинні проходити через один і той же NAT-маршрутизатор.

   При використанні декількох точок підключення до мережі, тре забезпечити синхронізацію усіх маршрутизаторів NAT, щоб при виході з ладу одного маршрутизатора сеанс не обривався.

   Трансляція адрес не завжди прозора для застосунків, і в цих випадках треба застосовувати шлюзи прикладного рівня ALG. Застосунки, що вимагають втручання ALG, не повинні шифрувати свій трафік, якщо тільки не надавати ALG ключ для розшифровки трафіку.

   Технологія IPSec не працюватиме через NAT, так як протоколи, які використовуються цією технологією використовують хеш-суми для перевірки цілісності пакетів, а при обчисленні цієї хеш-суми беруться до уваги також і ті поля, які підміняються NATом.

3. Сутність механізму трансляції адрес і номерів портів.

   При проходженні пакета з внутрішньої в зовнішню мережу кожній парі {внутрішня приватна адреса; номер порту TCP / IP відправника} ставиться у відповідність інша пара {глобальна IP-адреса зовнішнього інтерфейсу; призначений номер порту TCP / IP}. Призначений номер порту вибирається довільно, але він повинен бути унікальним в межах усіх вузлів, які отримують вихід в зовнішню мережу. Відповідність фіксується в таблиці.

4. В яких випадках доцільно застосовувати базову технологію NAT?

   Базова технологія NAT забезпечує однозначне бієктивне відображення внутрішніх адрес у зовнішнє. Таким чином, базову технологію NAT є сенс використовувати, коли кількість внутрішніх адрес, які повинні мати доступ до мережі менша або така ж, як і кількість зовнішніх адрес.

5. Особливості роботи NAT для протоколу ICMP.

   Для протоколу керуючих повідомлень ICMP робота NAT не є прозорою. ICMP забезпечує зворотний зв'язок для передачі повідомлень про помилки від проміжних маршрутизаторів мережі джерелу пакета, який викликав помилку. Діагностичне повідомлення, що міститься в полі даних протоколу, включає IP-адреси і порти відправника і одержувача. При використанні NAT в якості таких адрес і портів будуть виступати не оригінальні адреси, а відображені. При надходженні пакета ICMP на прикордонний пристрій протоколу NAT недостатньо виконати тільки стандартну процедуру відображення адрес, необхідно скорегувати і вміст поля даних, замінивши і в ньому IP-адреси і номер порту. Ще однією особливістю NAT при обробці повідомлень ICMP є неможливість застосування портів TCP / UDP для відображення адрес, оскільки ці повідомлення передаються по мережі, упакованими безпосередньо в пакети IP без використання транспортних протоколів TCP і UDP. У такому випадку роль номерів портів виконують ідентифікатори запитів ICMP.

6. Яким чином в NAPT можна забезпечити доступ із зовнішньої мережі (ініціатор обміну) до деякого вузла внутрішньої мережі?

   За допомогою механізму перенаправлення портів, при якому на зовнішньому інтерфейсі маршрутизатора вікривається порт і усі пакети, які надсилаються на цей порт перенаправляються на заданий порт внутрішнього вузла мережі.

7. Чому під час налаштування сервера NAT обов'язково потрібно включити функцію шлюзу?

Функцію шлюзу необхідно увімкнути для того, щоб передавати трафік, який приходить на інтерфейси у внутрішній мережі у зовнішню мережу через відповідні інтерфейси і навпаки. Без увімкненої функції шлюзу передача трафіку між інтерфейсами неможлива.

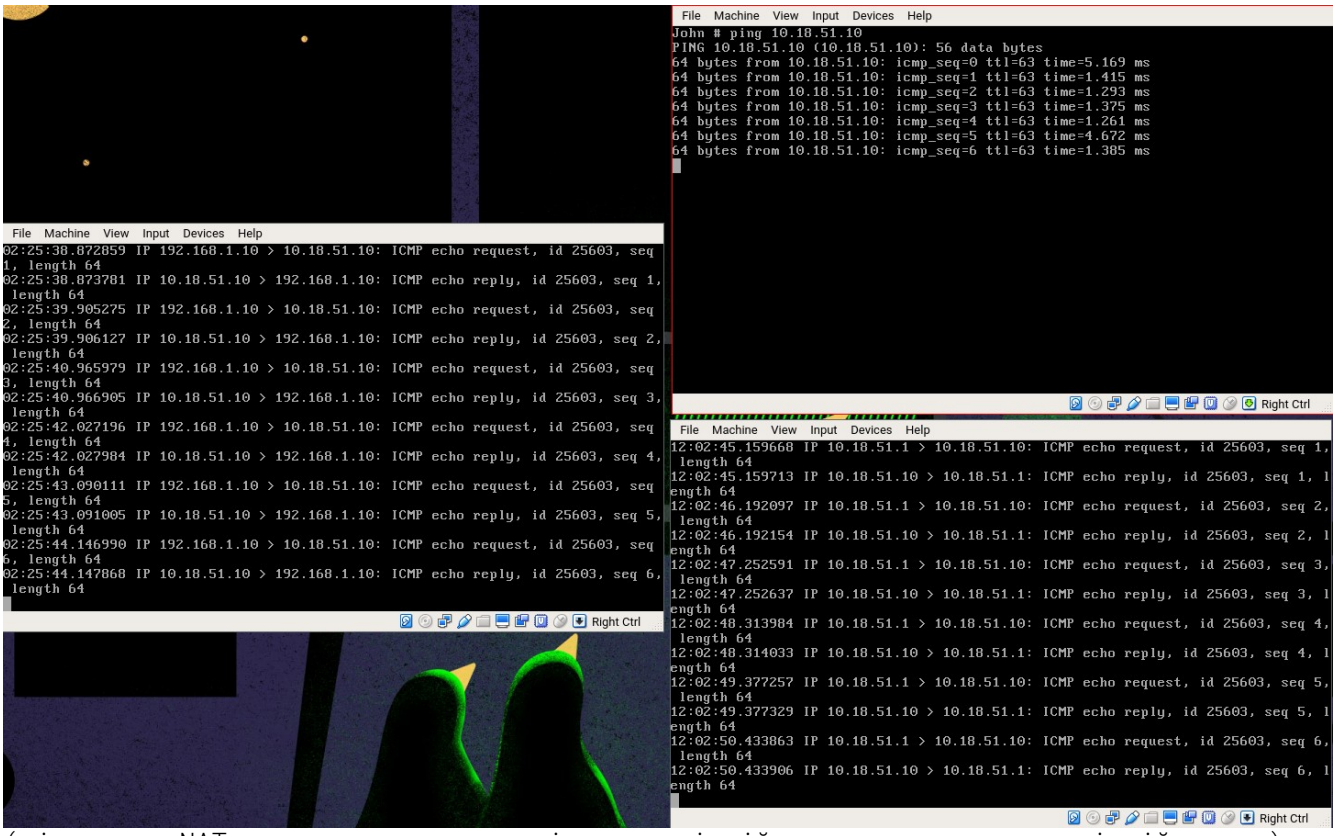
Налаштування маршрутизатора NAT

```
#!/bin/sh

# ============================
# Configure Address Translation
# ============================
echo << 'EOF' >/etc/firewall
#!/bin/sh
ipfw -q flush

# First we just passthrough packets to 25th port as is
ipfw -q add 00100 allow all from 192.168.1.10 to 10.18.51.0/24 25

# For other packets from 192.168.1.10 to 10.18.51.0 do address translation
ipfw -q add 00200 divert natd all from 192.168.1.10 to 10.18.51.0/24 via em1
ipfw -q add 00300 divert natd all from any to me via em1
EOF

# ========================
# Configure Port Forwarding
# ========================
echo << 'EOF' >/etc/natd.conf
redirect_port tcp 192.168.1.10:143 143
redirect_port tcp 192.168.1.10:110 110
EOF


# ============================
# Run all the things at startup
# ============================
echo << 'EOF' >/etc/rc.conf
#!/bin/sh
# internal network
ifconfig_em0="inet 192.168.1.1/24"
# external IP address
ifconfig_em1="inet 10.18.51.1/24"
hostname="olya"
sshd_enable="YES"

firewall_enable="YES"
firewall_nat_enable="YES"
firewall_gateway="YES"
gateway_enable="YES"
dummynet_enable="YES"
firewall_script="/etc/firewall"

natd_enable="YES"
natd_interface="em1"
natd_flags="-f /etc/natd.conf"
EOF

# ==============
# Troubleshouting
```

```
# ===============
# If the configuration above does not work
# You probably need to enable NAT support in Kernel
# as well as ensure your firewall allows all packets by default
# To do so, build the kernel with following options:
#
# options     IPFIREWALL
# options     IPFIREWALL_DEFAULT_TO_ACCEPT
# options     IPFIREWALL_VERBOSE
# options     IPFIREWALL_VERBOSE_LIMIT=100
# options     IPDIVERT
# options     DUMMYNET
```

Налаштування внутрішнього вузла мережі

```
#!/bin/sh

# ======================================
# Configure ip address and default gateway
# ======================================
cat << 'EOF' >/etc/rc.conf
#!/bin/sh
ifconfig_em0="inet 192.168.1.10/24"
defaultrouter="192.168.1.1"
hostname="john"
EOF
```



(ліворуч – NAT-маршрутизатор, вгорі – внутрішній вузол, внизу – зовнішній вузол)