T: Podłączanie sieci prywatnych do Internetu: NAT, firewall, proxy.

Sieci lokalne podłączamy do Internetu za pośrednictwem routerów. Router pełnią rolę bramy internetowej przez którą przechodzą wszystkie dane pomiędzy siecią lokalną a Internetem. Aby możliwe było połączenie z Internetem musimy posiadać co najmniej jeden publiczny adres IP. Od strony Internetu sieć lokalna widziana jest pod tym jednym adresem IP.

Zadanie1:

Wykorzystując serwis internetowy Wikipedii wyjaśnij pojęcia NAT, firewall i proxy.

Wyróżniamy następujące translacje adresów:
- translacja adresów źródłowych (SNAT – Source NAT),
- translacja adresów docelowych (DNAT – Destination NAT).

Zapora sieciowa (firewall) służy do zabezpieczania sieci i systemów przed nieuprawnionym dostępem z sieci komputerowych. Filtrowanie danych może polegać na akceptowaniu lub odrzucaniu połączeń według:
- warstwy dostępu do sieci (źródłowe i docelowe adresy MAC),
- warstwy sieciowej (adresy IP nadawcy i odbiorcy),
- warstwy transportowej (porty źródłowe i docelowe usług internetowych),
- warstwy aplikacji (protokoły usług internetowych).

Serwer pośredniczący (proxy) łączy użytkownika z siecią, przez co może ukrywać informacje o użytkowniku (IP, nazwa użytkownika, używane oprogramowanie) oraz buforuje pobierane dane.

Zadanie2:

Czy w szkolnej sieci komputerowej znajdują się serwery NAT, firewall i proxy?

Zadanie3:

Wykonaj poniższe polecenie i przeanalizuj uzyskane wyniki:

```
traceroute wp.pl
tracert wp.pl
```

Zadanie4:

W jaki sposób wykorzystałbyś w swojej sieci serwery NAT, firewall i proxy?

Rodzaje serwerów proxy:
- **high anonymous** (całkowicie anonimowe, zwane też elite proxy) - serwer nie wysyła żadnych wiadomości o użytkowniku, także tego że korzysta z serwera proxy,
- **anonymous** (anonimowe) serwer nie wysyła żadnych wiadomości o użytkowniku, ale zgłasza się jako serwer proxy u odbiorcy,
- **transparent** (przeźroczyste) - utajniają dane o użytkowniku, ale nie ukrywają adresu IP. Jedyną zaletą jest możliwość korzystania z cache'u.

Zadanie5:

Odwiedź następujące witryny internetowe: `http://multiproxy.org` oraz `http://lista-proxy.net`.

Ciekawe spostrzeżenia:

`http://proxyb:port/http://proxyc:port/http://www.strona.com`

Zadanie6:

W grupach dwuosobowych należy skonfigurować połączenie sieciowe w taki sposób, aby jedno stanowisko udostępniało połączenie drugiemu. Ćwiczenie należy wykonać w systemie Linux bez dodawania dodatkowych urządzeń sieciowych i modyfikowania plików konfiguracyjnych.

Rozwiązanie (pracujemy na koncie root):

Czynności wykonane na serwerze (stanowisko nieparzyste):

- w celu ominięcia problemów z firewall-em należy na czas ćwiczenia wyłączyć zabezpieczenia oraz zdefiniować translację adresów NAT:
```
/sbin/iptables -F
/sbin/iptables -P INPUT ACCEPT
/sbin/iptables -P FORWARD ACCEPT
/sbin/iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE
```
- konfigurujemy dodatkowy adres IP dla karty sieciowej:
```
ifconfig eth0:1 192.168.9.1 netmask 255.255.255.0
```
- włączamy przekazywanie pakietów:
```
echo "1" > /proc/sys/net/ipv4/ip_forward
```
- sprawdzamy dokonane ustawienia poleceniami:
```
ifconfig
route -n
```
- włączamy nasłuch na karcie sieciowej:
```
tcpdump
```

Czynności wykonane na kliencie (stanowisko parzyste):

- wyłączamy kartę sieciową w celu usunięcia poprzedniego numeru IP:
```
ifconfig eth0 down
```
- włączamy kartę sieciową z nową konfiguracją IP:
```
ifconfig eth0 192.168.9.2 netmask 255.255.255.0
```
- dodajemy nową domyślną bramkę internetową:
```
route add default gw 192.168.9.1
```
- sprawdzamy dokonane ustawienia poleceniami:
```
ifconfig
route -n
```
- sprawdzamy funkcjonowanie połączenia:
```
ping 212.77.100.101
ping wp.pl
```
- możemy dodać konfigurację serwera DNS w przypadku problemów z adresami domenowymi:
```
echo "nameserver 194.204.152.34" >> /etc/resolv.conf
```

Zakończenie:

- resetujemy dokonane zmiany poleceniem na obu komputerach:
```
/etc/init.d/network restart
```