Wydział Informatyki Laboratorium Sieci Komputerowych	Data: 19.01.2021 r.
Sprawozdanie z Projektu Zespół: Krzysztof Kalinowski (lider) Gabriel Chomiczewski Łukasz Chojecki Jakub Snarski Tomasz Sokołowski Grupa: LAB13	 Prowadzący: dr. inż. Walenty Oniszczuk Ocena:

1. Zadanie

Należało skonfigurować sieć komputerową w małej firmie. Firma ma piwnicę, parter i piętro. Na parterze oraz na piętrze pracują graficy, programiści oraz kierownik, natomiast w piwnicy mamy serwerownię. Dodatkową informacją jest to, że nie możemy wykonywać nawierceń w stropie pomiędzy piwnicą a parterem. Mamy za zadanie zapewnić dostęp do Internetu dla wszystkich pracowników, podzielić grupy różnych pracowników na podsieci, postawić serwer WWW firmy, router Wi-Fi dla kierowników oraz firewall dla pracowników.

2. Schemat sieci

<tutaj schemat>

3. Podział adresów IP

<tutaj podział adresów IP>

4. Realizacja zadania

W celu łatwiejszego poruszania się po dokumentacji z projektu zadanie możemy podzielić na fazy, które składają się na końcowy wynik, w postaci poprawnie działającej sieci komputerowej.

- **Faza I: Serwerownia**

Zgodnie z planem w piwnicy naszej firmy postanowiliśmy postawić serwer WWW oraz uzyskać połączenie z siecią zewnętrzną. W celu tego uzyskania tego drugiego musieliśmy skonfigurować serwer DHCP na mikrotiku. Podłączamy przewód do odpowiedniego interfejsu, następnie ustawiamy pulę adresów z której może zostać nam przydzielony przez serwer adres IP, dodajemy serwer i go uruchamiamy. Po tych akcjach przydzielony został nam adres:

<tutaj zdjecie adresu z DHCP mikrotik>

Aby zapewnić komunikację z innymi elementami naszej sieci ustawiliśmy wartość bramy domyślnej. Wykorzystaliśmy także inne porty tego urządzenia: jeden ether dla połączenia się z serwerem WWW oraz jeden bezprzewodowy, w celu połączenia się z parterem bez wykonywania dodatkowych nawierceń w stropie.

<tutaj zdjecie adresow na portach mikrotik>

Nasz serwer, poza samym serwerem WWW, musi posiadać także skonfigurowane DHCP, aby strona naszej firmy była widoczna również w sieci rozległej, aby potencjalni klienci mogli z niej korzystać. W taki sposób prezentuje się plik konfiguracyjny interfejsów serwera.

```
# interfaces(5) file used by ifup(8) and ifdown(8)

auto lo
iface lo inet loopback

auto eth1
iface eht1 dhcp

auto eth0
iface eth0 inet static
address 192.168.10.196
netmask 255.255.255.0
```

Po zrestartowaniu serwera widzimy, że przydzielił on nam IP z zadanej puli. Drugą częścią, jeśli chodzi o serwer WWW jest konfiguracja samego Apache. Strona musi zawierać zasoby publiczne, dla klientów oraz zasoby prywatne, do których mają dostęp tylko i wyłącznie pracownicy z komputerów, które mają w pracy. Zasoby prywatne dodatkowo chronione są hasłami dostępu. W taki sposób wygląda struktura katalogów zawierających dane do poszczególnych zasobów.

```
Net4
├── index.html
└── private
    ├── hasla.txt
    └── index.html
```

Musieliśmy dodatkowo nanieść poprzednie zmiany w pliku konfiguracyjnym serwera, aby zapewnić między innymi wspomniany wcześniej dostęp do zasobów prywatnych po podaniu hasła oraz tylko z komputera z sieci firmowej. Poniżej znajduje się kod znajdujący się w pliku konfiguracyjnym.

<kod z pliku konfiguracyjnego>

Serwer dodatkowo podpięty jest do mikrotika, który przekierowuje dostęp do serwera lokalnie na parter. Po konfiguracji komponentów znajdujących się dalej w sprawozdaniu, mogliśmy zauważyć, iż mamy lokalnie dostęp do serwera, po wpisaniu w przeglądarkę jego adresu lokalnego.

<zdjecie z strona i adresem danym dla serwera>

- **Faza II: Mikrotik na parterze oraz przełączniki**

Aby zapewnić dalszy dostęp do Internetu w naszej firmie, potrzebowaliśmy użyć drugiego mikrotika na piętrze, aby ten przechwycił sygnał z piwnicy oraz przekazał go dalej do przełącznika. Wykorzystaliśmy fakt, że mikrotik ma 3 interfejsy typu ether i postanowiliśmy podzielić na jego poziomie podzielić sieć na podsieci: programistów, grafików oraz kierowników. W taki sposób prezentowały się adresy na poszczególnych interfejsach mikrotika

<zdjecie mikrotik gorny adresy>

Do naszego projektu wykorzystaliśmy dwa przełączniki zarządzalne: jeden na parterze, drugi na piętrze. Poszczególne porty zostały podzielone na VLANy, tak aby dodatkowo oddzielić od siebie różne grupy pracowników. Switche zostały ze sobą połączone przy użyciu portów 24, oznaczyliśmy je jako porty tagowane, co umożliwia przesyłanie sygnału pomiędzy piętrami, przy wykonaniu

pojedyńczego nawiercenia w suficie. Poniżej znajduje się rozpis jak podzielone zostały porty na poszczególnych switchach.

<zdjecia dwa z vlanami>

Najważniejszy jest jednak sam wynik, wykonywanej operacji. Poniżej znajdują się wyniki testu operacji ping dla testu komunikacji z komputerem z tego samego piętra z tej samej podsieci, z komputerem z innej podsieci oraz komunikację pomiędzy piętrami.

<foty pingów>

- **Faza III: Router dla kierownika oraz firewall**

Zgodnie z wymaganiami, potrzebujemy bezprzewodowego punktu dostępu do Internetu dla kierowników. W tym celu na parterze do jednego z portów sieci VLAN kierowników, podłączony został skonfigurowany router Wi-Fi. Nadany mu został adres statyczny, tak aby adres należał do podsieci kierowników, natomiast dostęp do niego został zabezpieczony hasłem.

<może jakis screen>

Ostatnia czynnością jest konfiguracja firewalla. Zdecydowaliśmy się na konfigurację firewalli na komputerach programistów oraz grafików. Jest to wystarczające rozwiązanie zważywszy na to, że nowe komputery jakie będą pojawiać się w firmie, to komputery kierowników, a na te komputery nie musimy nakładać żadnego ogarniczenia. Poniżej znajdują się zawartości plików konfiguracji tej usługi.

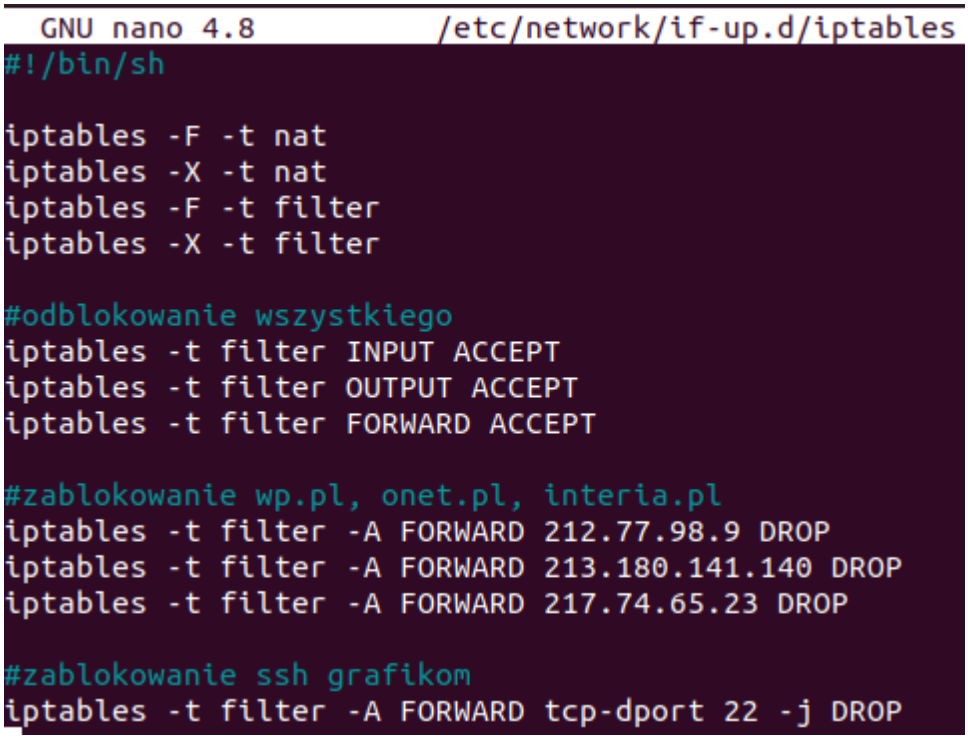
```
  GNU nano 4.8          /etc/network/if-up.d/iptables
#!/bin/sh

iptables -F -t nat
iptables -X -t nat
iptables -F -t filter
iptables -X -t filter

#odblokowanie wszystkiego
iptables -t filter INPUT ACCEPT
iptables -t filter OUTPUT ACCEPT
iptables -t filter FORWARD ACCEPT

#zablokowanie wp.pl, onet.pl, interia.pl
iptables -t filter -A FORWARD 212.77.98.9 DROP
iptables -t filter -A FORWARD 213.180.141.140 DROP
iptables -t filter -A FORWARD 217.74.65.23 DROP
```

Firewall dla programistów (brak blokady ssh -> portu 22)



Firewall grafików (blokada ssh -> portu 22)

5. Wnioski:

Cała sieć firmy, działała w poprawny sposób oraz spełnione zostały wszystkie założenia:

-wszyscy pracownicy mają dostęp do internetu

-programiści oraz graficy mają nałożone odpowiednie ograniczenia przeglądania

-wszyscy pracownicy mają lokalny dostęp do serwera WWW firmy, który posiada zasoby prywatne i publiczne

-komputery pracowników mają własne podsieci przez co możliwa jest komunikacja tylko pomiędzy użytkownikami tej samej grupy.

Przedstawiony sposób realizacji projektu został zaakceptowany przez prowadzącego.