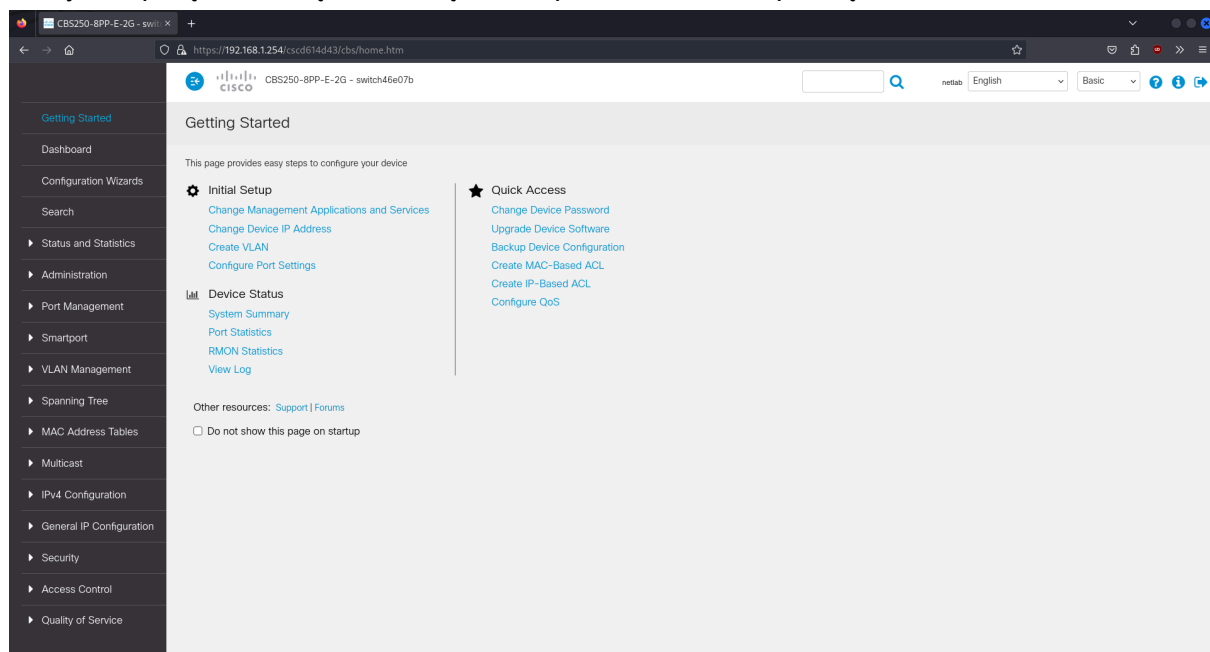


Instalacja usługi DHCP na naszym komputerze serwerowym

```
(root@sala201-202)-[/home/student]
# apt-get install isc-dhcp-server
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
isc-dhcp-server is already the newest version (4.4.3-P1-4).
The following packages were automatically installed and are no longer required:
  ettercap-common ettercap-graphical liblua5.1-2 liblua5.1-common
  python3-qrcode
Use 'sudo apt autoremove' to remove them.
0 upgraded, 0 newly installed, 0 to remove and 1230 not upgraded.
```

Pomyślne połączenie się ze stroną Cisco, po zresetowaniu przełącznika



Ustawiliśmy eth0 na interfejs sieciowy 192.168.1.4 w tej samej podsieci co przełącznik cisco

```
(student@sala201-202)-[~]
$ sudo ifconfig eth0 192.168.1.4
```

Ustawienie truncate na 10 porcie przełącznika cisco

Interface Settings Table



Filter: *Interface Type* equals to

Port ▾

Go

	Entry No.	Interface	Interface VLAN Mode
<input type="radio"/>	1	GE1	Access
<input type="radio"/>	2	GE2	Access
<input type="radio"/>	3	GE3	Access
<input type="radio"/>	4	GE4	Access
<input type="radio"/>	5	GE5	Access
<input type="radio"/>	6	GE6	Access
<input type="radio"/>	7	GE7	Access
<input type="radio"/>	8	GE8	Access
<input type="radio"/>	9	GE9	Access
<input type="radio"/>	10	GE10	Trunk

Podzielenie VLAN'ów na grupy na Cisco, przy czym port szefa ma id 10, programiści mają id 20, a graficy mają id 30.

VLAN Settings

VLAN Table



<input type="checkbox"/>	VLAN ID	VLAN Name	Originators	VLAN Interface State	Link Status SNMP Traps
<input type="checkbox"/>	1		Default	Enabled	Enabled
<input type="checkbox"/>	10	szefg	Static	Enabled	Enabled
<input type="checkbox"/>	20	programiscig	Static	Enabled	Enabled
<input type="checkbox"/>	30	graficyg	Static	Enabled	Enabled

Przypisanie VLAN'ów do konkretnych portów przełącznika, gdzie szef ma port 2 , programiści 2 porty 3 i 4, a graficy 2 porty 5 i 6

Port VLAN Membership

F - Forbidden member T - Tagged member U - Untagged member I - Inactive VLAN F
In - Internally used VLAN

Port VLAN Membership Table

Join VLAN...Details...

Filter: *Interface Type* equals to

Port

Go

	Interface	Mode	Administrative VLANs	Operational VLANs	LAG
<input type="radio"/>	GE1	Access	1U	1U	
<input type="radio"/>	GE2	Access	10U	10U	
<input type="radio"/>	GE3	Access	20U	20U	
<input checked="" type="radio"/>	GE4	Access	20U	20U	
<input type="radio"/>	GE5	Access	30U	30U	
<input type="radio"/>	GE6	Access	30U	30U	
<input type="radio"/>	GE7	Access	1U	1U	
<input type="radio"/>	GE8	Access	1U	1U	
<input type="radio"/>	GE9	Access	1U	1U	
<input type="radio"/>	GE10	Trunk	1U, 2-9I, 10T, 11-19I, 20...	1U, 10T, 20T, 30T	

Połączenie się przez truncate pomiędzy Cisco a Mikrotikiem i ustawienie grup na Mikrotiku, żeby dwa przełączniki były podobnie skonfigurowane co do portów na każdym piętrze.

5 items											
	Name	Type	MTU	Actual MTU	L2 MTU	Tx	Rx	Tx Packet (p/s)	Rx Packet (p/s)	FP Tx	F
<div><div></div><div></div></div>	graficy1d	VLAN	1500	1500	1594	0 bps	0 bps	0	0	0 bps	0
<div><div></div><div></div></div>	graficy2d	VLAN	1500	1500	1594	0 bps	0 bps	0	0	0 bps	0
<div><div></div><div></div></div>	programisci1d	VLAN	1500	1500	1594	0 bps	0 bps	0	0	0 bps	0
<div><div></div><div></div></div>	programisci2d	VLAN	1500	1500	1594	0 bps	0 bps	0	0	0 bps	0
<div><div></div><div></div></div>	szef1d	VLAN	1500	1500	1594	0 bps	0 bps	0	0	0 bps	0

DHCP

Zainstalowaliśmy usługę DHCP używając polecenia:

```
sudo apt-get install isc-dhcp-server
```

Stworzyliśmy podsieci w pliku /etc/dhcp/dhcpd.conf

```
GNU nano 7.2 /etc/dhcp/dhcpd.conf
subnet 10.64.104.0 netmask 255.255.255.0 {
    range 10.64.104.10 10.64.104.100;
    option routers 10.64.104.216; # IP address of eth0
    option broadcast-address 10.64.104.255;
}

subnet 192.168.10.0 netmask 255.255.255.0 {
    range 192.168.10.50 192.168.10.150;
    option routers 192.168.10.1; # IP address of eth0:1 (if applicable)
}

subnet 192.168.20.0 netmask 255.255.255.0 {
    range 192.168.20.50 192.168.20.150;
    option routers 192.168.20.1; # IP address of eth0:2 (if applicable)
}

subnet 192.168.30.0 netmask 255.255.255.0 {
    range 192.168.30.50 192.168.30.150;
    option routers 192.168.30.1; # IP address of eth0:3 (if applicable)
}
```

Po czym włączyliśmy usługę

Apache

Instalacja:

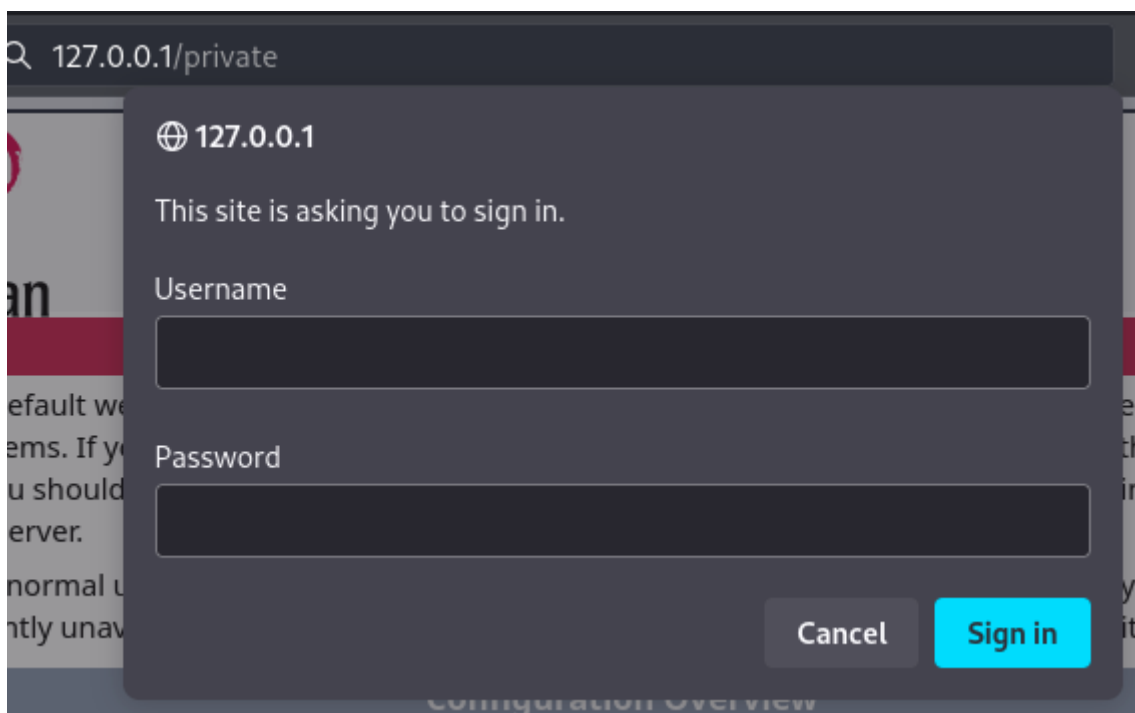
```
apt-get install apache2 apache2-utils apache2-bin apache2-data
```

```
Do /etc/apache2/sites-enabled/000-default.conf dodaje Alias /oceny  
"/var/klienci/index.html"
```

Dodaje katalog:

```
mkdir /var/www/klienci
```

```
<VirtualHost *:80>  
    # The ServerName directive sets the request scheme, hostname and port that  
    # the server uses to identify itself. This is used when creating  
    # redirection URLs. In the context of virtual hosts, the ServerName  
    # specifies what hostname must appear in the request's Host: header to  
    # match this virtual host. For the default virtual host (this file) this  
    # value is not decisive as it is used as a last resort host regardless.  
    # However, you must set it for any further virtual host explicitly.  
    #ServerName www.example.com  
  
    ServerAdmin webmaster@localhost  
    DocumentRoot /var/www/html  
    Alias /klienci "/var/www/klienci/index.html"  
    Alias /private "/var/www/private"  
  
    # Available loglevels: trace8, ..., trace1, debug, info, notice, warn,  
    # error, crit, alert, emerg.  
    # It is also possible to configure the loglevel for particular  
    # modules, e.g.  
    #LogLevel info ssl:warn  
  
    ErrorLog ${APACHE_LOG_DIR}/error.log  
    CustomLog ${APACHE_LOG_DIR}/access.log combined  
  
    <Directory "/var/www/private">  
        AuthType Basic  
        AuthName "Wprowadz haslo"  
        AuthUserFile "/var/www/private/password.txt"  
        Require user testowy  
    </Directory>  
  
    # For most configuration files from conf-available/, which are  
    # enabled or disabled at a global level, it is possible to  
    # include a line for only one particular virtual host. For example the  
    # following line enables the CGI configuration for this host only  
    # after it has been globally disabled with "a2disconf".  
    #Include conf-available/serve-cgi-bin.conf  
</VirtualHost>
```



127.0.0.1/private/			
<h1>Index of /private</h1>			
	<u>Name</u>	<u>Last modified</u>	<u>Size Description</u>
	Parent Directory		-
	password.txt	2024-01-11 14:27	46
<hr/>			
<i>Apache/2.4.58 (Debian) Server at 127.0.0.1 Port 80</i>			

Serwer FTP

Zainstalowaliśmy usługę używając komendy `apt install vsftpd -y`

```
(root@sala201-202)-[/home/student]
# apt install vsftpd -y
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
vsftpd is already the newest version (3.0.3-13+b3).
The following packages were automatically installed and are no longer required:
  ettercap-common ettercap-graphical libluajit-5.1-2 libluajit-5.1-common python3-qrcode
Use 'sudo apt autoremove' to remove them.
0 upgraded, 0 newly installed, 0 to remove and 1230 not upgraded.

(root@sala201-202)-[/home/student]
# nano /etc/vsftpd/vstfpd.conf
```

Następnie otworzyliśmy poniższy plik przy pomocy nano

```
(root@sala201-202)-[/home/student]
# nano /etc/vsftpd.conf
```

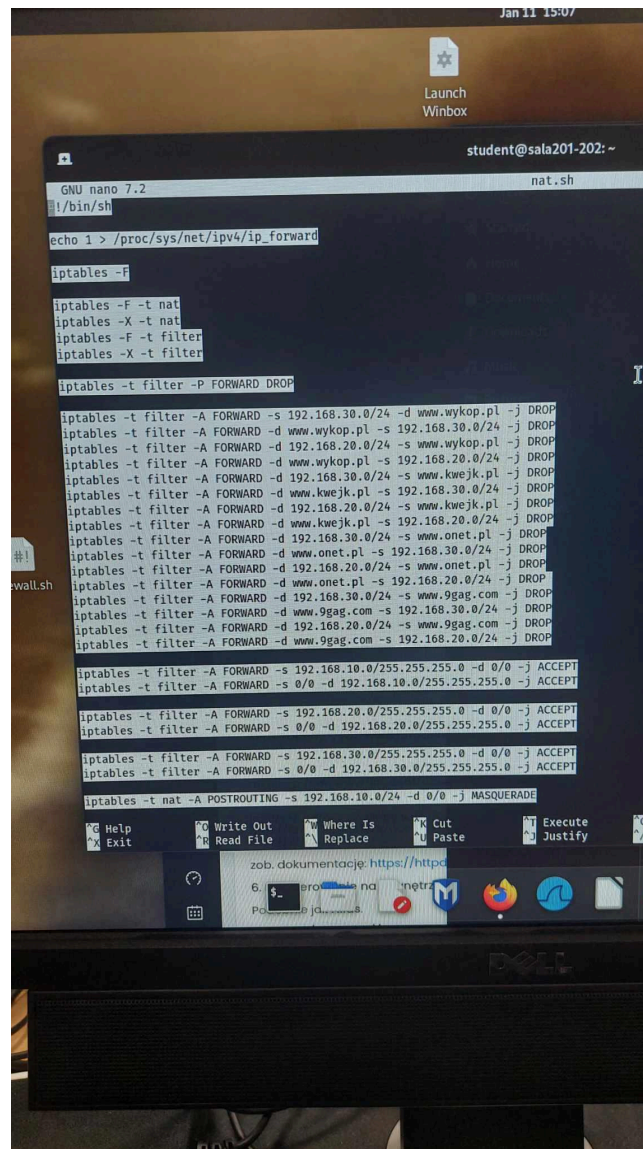
```
# Example config file /etc/vsftpd.conf
#
# The default compiled in settings are fairly paranoid. This sample file
# loosens things up a bit, to make the ftp daemon more usable.
# Please see vsftpd.conf.5 for all compiled in defaults.
#
# READ THIS: This example file is NOT an exhaustive list of vsftpd options.
# Please read the vsftpd.conf.5 manual page to get a full idea of vsftpd's
# capabilities.
#
# Run standalone? vsftpd can run either from an inetd or as a standalone
# daemon started from an initscript.
listen=NO
#
# This directive enables listening on IPv6 sockets. By default, listening
# on the IPv6 "any" address (::) will accept connections from both IPv6
# and IPv4 clients. It is not necessary to listen on *both* IPv4 and IPv6
# sockets. If you want that (perhaps because you want to listen on specific
# addresses) then you must run two copies of vsftpd with two configuration
# files.
listen_ipv6=YES
#
# Allow anonymous FTP? (Disabled by default).
anonymous_enable=NO
#
# Uncomment this to allow local users to log in.
local_enable=YES
#
# Uncomment this to enable any form of FTP write command.
write_enable=YES
#
# Default umask for local users is 077. You may wish to change this to 022,
# if your users expect that (022 is used by most other ftpd's)
local_umask=022
#
# Uncomment this to allow the anonymous FTP user to upload files. This only
# has an effect if the above global write enable is activated. Also, you will
# obviously need to create a directory writable by the FTP user.
anon_upload_enable=YES
#
# Uncomment this if you want the anonymous FTP user to be able to create
# new directories.
anon_mkdir_write_enable=YES
#
# Activate directory messages - messages given to remote users when they
# go into a certain directory.
dirmessage_enable=YES
#
```

Nastąpiła domyślna konfiguracja serwera ftp. Następnie zrestartowaliśmy serwer używając polecenia `restart vsftpd` oraz wyświetliliśmy status

```
(root@sala201-202)-[/home/student]
# systemctl restart vsftpd

(root@sala201-202)-[/home/student]
# systemctl status vsftpd
● vsftpd.service - vsftpd FTP server
   Loaded: loaded (/lib/systemd/system/vsftpd.service; disabled; preset: disabled)
   Active: active (running) since Thu 2024-01-11 14:50:47 GMT; 9s ago
     Process: 18489 ExecStartPre=/bin/mkdir -p /var/run/vsftpd/empty (code=exited, status=0/SUCCESS)
    Main PID: 18491 (vsftpd)
       Tasks: 1 (limit: 18892)
      Memory: 1.0M
         CPU: 18ms
    CGroup: /system.slice/vsftpd.service
            └─18491 /usr/sbin/vsftpd /etc/vsftpd.conf
```

Firewall oraz Maskarada



```
Jan 11 15:07
Launch
Winbox
student@sala201-202: ~
nat.sh
GNU nano 7.2
#!/bin/sh

echo 1 > /proc/sys/net/ipv4/ip_forward

iptables -F

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

iptables -t filter -P FORWARD DROP

iptables -t filter -A FORWARD -s 192.168.30.0/24 -d www.wykop.pl -j DROP
iptables -t filter -A FORWARD -d www.wykop.pl -s 192.168.30.0/24 -j DROP
iptables -t filter -A FORWARD -d 192.168.20.0/24 -s www.wykop.pl -j DROP
iptables -t filter -A FORWARD -d www.wykop.pl -s 192.168.20.0/24 -j DROP
iptables -t filter -A FORWARD -d 192.168.30.0/24 -s www.kwejk.pl -j DROP
iptables -t filter -A FORWARD -d www.kwejk.pl -s 192.168.30.0/24 -j DROP
iptables -t filter -A FORWARD -d 192.168.20.0/24 -s www.kwejk.pl -j DROP
iptables -t filter -A FORWARD -d www.kwejk.pl -s 192.168.20.0/24 -j DROP
iptables -t filter -A FORWARD -d 192.168.30.0/24 -s www.onet.pl -j DROP
iptables -t filter -A FORWARD -d www.onet.pl -s 192.168.30.0/24 -j DROP
iptables -t filter -A FORWARD -d 192.168.20.0/24 -s www.onet.pl -j DROP
iptables -t filter -A FORWARD -d www.onet.pl -s 192.168.20.0/24 -j DROP
iptables -t filter -A FORWARD -d 192.168.30.0/24 -s www.9gag.com -j DROP
iptables -t filter -A FORWARD -d www.9gag.com -s 192.168.30.0/24 -j DROP
iptables -t filter -A FORWARD -d 192.168.20.0/24 -s www.9gag.com -j DROP
iptables -t filter -A FORWARD -d www.9gag.com -s 192.168.20.0/24 -j DROP

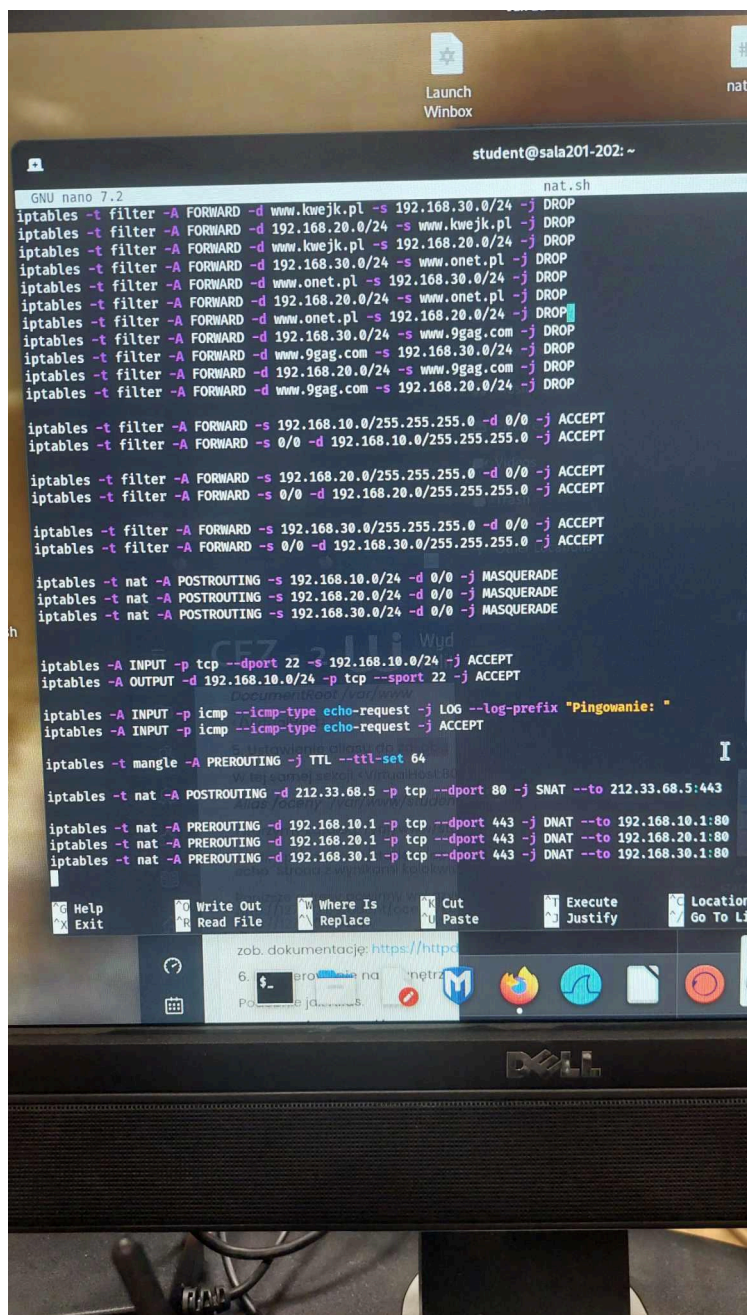
iptables -t filter -A FORWARD -s 192.168.10.0/255.255.255.0 -d 0/0 -j ACCEPT
iptables -t filter -A FORWARD -s 0/0 -d 192.168.10.0/255.255.255.0 -j ACCEPT

iptables -t filter -A FORWARD -s 192.168.20.0/255.255.255.0 -d 0/0 -j ACCEPT
iptables -t filter -A FORWARD -s 0/0 -d 192.168.20.0/255.255.255.0 -j ACCEPT

iptables -t filter -A FORWARD -s 192.168.30.0/255.255.255.0 -d 0/0 -j ACCEPT
iptables -t filter -A FORWARD -s 0/0 -d 192.168.30.0/255.255.255.0 -j ACCEPT

iptables -t nat -A POSTROUTING -s 192.168.10.0/24 -d 0/0 -j MASQUERADE

Help Write Out Where Is Cut Execute
Exit Read File Replace Paste Justify
zob. dokumentacje: https://httpd
6. ... na ... netr
Pobierz ...
```



Napisaliśmy skrypt firewalla który odcina dostęp do stron: www.9gag.com, www.onet.pl, www.kwejk.pl oraz www.wykop.pl. przy czym szefowie mają dostęp.

Zadania	Punktacja
Skonfigurować dostęp do Internetu dla wszystkich pracowników. Zakładamy, że większość pracowników nie jest w stanie samodzielnie skonfigurować interfejsów sieciowych. W związku z tym, wszelkie parametry powinny być konfigurowane w sposób automatyczny, bez jakiegokolwiek ingerencji pracowników.	1pkt (2 pkt.)
Firma chciałaby mieć swój własny serwer WWW, z którego mogliby korzystać wszyscy aktualni i potencjalni klienci.	0.4 (0.4 pkt.)
Część zasobów serwera WWW powinna być ogólnodostępna, natomiast dostęp do pozostałych zasobów powinien być możliwy tylko dla pracowników firmy, ale tylko wtedy, gdy korzystają oni z komputerów znajdujących się wewnątrz sieci firmowej.	0.4 (0.4 pkt.)
Niestety, do chwili obecnej nie wykupili jeszcze żadnej domeny; dopuszcza się więc możliwość korzystania tylko z adresów IP. Ponadto, każdy z pracowników chce mieć własną przestrzeń na serwerze WWW, którą mogliby dowolnie konfigurować. Wyjątkiem są szefowie o loginach: szef1 oraz szef2, którzy nie są tym zainteresowani i nawet gdyby próbowali udostępniać jakieś dokumenty, dostęp powinien być zabroniony.	0 (0.4 pkt)
Każda z podsieci pracowników, powinna być odseparowana od innych, tzn. dostęp do urządzeń z innej podsieci powinien być zablokowany.	0.4 (1.2 pkt.)
Szefowie korzystają czasami z dodatkowych komputerów przenośnych, które wewnątrz firmy powinny mieć takie same uprawnienia jak ich urządzenia stacjonarne.	0 (1 pkt.)
przeglądania zawartości wszystkich stron WWW, ale z pewnymi wyjątkami. Pracownicy zbyt dużo czasu spędzają czytając zawartość portali internetowych: www.9gag.com, www.onet.pl, www.kwejk.pl oraz www.wykop.pl. W związku z tym, należy „odciąć” im dostęp z sieci lokalnej (szefowie powinni mieć dostęp),	0.4 (0.4 pkt.)
korzystania z komunikatora,	0.2 (0.2 pkt.)

programiści powinni mieć możliwość łączenia się z zewnętrznymi serwerami poprzez SSH,	0.4 (0.4 pkt.)
szef grupy programistów chce mieć możliwość łączenia się z domu ze swoim firmowym komputerem za pomocą SSH.	0(0.6 pkt)
ponieważ istnieje uzasadnione podejrzenie o próbach skompromitowania głównego serwera, wszystkie próby „pingowania” powinny być logowane,	(0.4 pkt.)
pakiety wysyłane na zewnątrz powinny mieć identyczną wartość TTL, bez względu na to, czy zostały wysłane z serwera dostępowego, czy też urządzeń klienckich, pozostały ruch sieciowy powinien być zablokowany.	(0.4 pkt.)

W dalszej Perspektywie:

Zadania	Punktacja
O ile programiści, z racji tego, że są informatykami, mogą do komunikacji w sieci lokalnej korzystać z adresów IP, to pozostałym pracownikom sprawia to trudność. Jako bardziej przyjazne i łatwiejsze do zapamiętania wydają się im nazwy domenowe, z którymi zdążyli oswoić się korzystając z Internetu. Z racji liczby urządzeń w firmie, nieefektywne wydaje się „ręczne” konfigurowanie każdego z urządzeń .	(2 pkt)
Ze względu bezpieczeństwa dostęp do zasobu <code>http://<IPAddress>/secure</code> powinien być szyfrowany, a każdorazowe odwołanie za pomocą protokołu <code>http</code> , powinno skutkować wymuszaniem połączenia <code>https</code> .	(2 pkt.)
Potrzebny jest też serwer FTP, z którego dane mogłyby pobierać firmy współpracujące. Część zasobów powinna być udostępniona użytkownikom anonimowym (anonymous), pozostała - dostępna po autoryzacji .	(0.4 pkt.)
Każda z grup pracowników, tzn. szefowie, graficy i programiści, chciałaby mieć własny katalog wymiany (nie poprzez FTP), przez który pracownicy z danej grupy mogliby się wymieniać zasobami	(2 pkt.)

<p>plikowymi. Wymagane jest, aby dostęp do tego katalogu mieli tylko i wyłącznie pracownicy tej grupy. Ponadto, wymagany jest dodatkowy katalog wymiany, dostępny dla wszystkich pracowników i niewymagający autoryzacji. Taki katalog wymiany powinien być widoczny jako zwykły katalog w „otoczeniu sieciowym”. Dodatkowy problem stanowi fakt, że na jednym z laptopów szefa zainstalowane są systemy z rodziny Windows, a pozostali użytkownicy zwykle korzystają z różnych dystrybucji systemu Linux .</p>	
<p>Jednym z niewątpliwie niezbędnych do pracy narzędzi komunikacji jest serwer pocztowy</p>	<p>(2 pkt.)</p>
<p>najlepiej z dostępem poprzez przeglądarkę .</p>	<p>(1 pkt.)</p>
<p>Planowane jest również utworzenie oddziału w innym mieście. Pracownicy zdalni powinni mieć dostęp do wszystkich urządzeń w firmie macierzystej .</p>	<p>(2 pkt.)</p>