

Bezpieczeństwo sieci komputerowych

Sprawozdanie z laboratorium

Data	Tytuł zajęć	Uczestnicy
30.10.2018 09:15	Zapory ogniowe, filtrowanie ruchu	Igor Bejnarowicz (218573) Bartosz Rodziejwicz (226105)

Przebieg laboratorium

Zadanie laboratoryjne udało nam się zrealizować w bardzo ograniczonym zakresie z uwagi na kilka naszych niedopatrzeń. Najpierw mieliśmy problem z niedoczytaniem, że należy zapory zresetować do ustawień domyślnych, a następnie, że mieliśmy problem z kartą sieciową w Windowsie/maszynie wirtualnej.

Po rozwiązaniu problemu z brakiem domyślnej konfiguracji, połączyliśmy się z czystą zaporą i zapoznaliśmy się z domyślną konfiguracją.

Zapora posiada 8 portów, z czego 7 jest przypisanych do **Vlan1**, o nazwie **inside** (są to porty **e0/1 - e0/7**) o poziomie bezpieczeństwa **100**, jeden port jest przypisany do **Vlan2**, o nazwie **outside**, poziomie bezpieczeństwa **0** i jest to port **e0/0**.

```
Executing command: exit
Executing command: http server enable
Executing command: http 192.168.1.0 255.255.255.0 inside
Executing command: dhcpd address 192.168.1.5-192.168.1.36 inside
Executing command: dhcpd auto_config outside
Executing command: dhcpd enable inside
Executing command: logging asdm informational
Factory-default configuration is completed
ciscoasa(config)# enable
ERROR: % Incomplete command
ciscoasa(config)# end
ciscoasa# show int ip brief
Interface      IP-Address      OK? Method Status      Protocol
Ethernet0/0    unassigned     YES unset   up          up
Ethernet0/1    unassigned     YES unset   up          up
Ethernet0/2    unassigned     YES unset   up          up
Ethernet0/3    unassigned     YES unset   down        down
Ethernet0/4    unassigned     YES unset   down        down
Ethernet0/5    unassigned     YES unset   down        down
Ethernet0/6    unassigned     YES unset   down        down
Ethernet0/7    unassigned     YES unset   down        down
Internal-Data0/0 unassigned     YES unset   up          up
Internal-Data0/1 unassigned     YES unset   up          up
Vlan1          192.168.1.1    YES manual up          up
Vlan2          192.168.255.207 YES DHCP   up          up
Virtual0       127.1.0.1      YES unset   up          up
ciscoasa# show vlan
Use "show switch vlan" to view the vlans that have been assigned to Layer 2 switch ports.
ciscoasa# conf t
ciscoasa(config)# hos
ciscoasa(config)# hostname
ERROR: % Incomplete command
ciscoasa(conhostname Rodziejwicz-Bejnarowicz
Rodziejwicz-Bejnarowicz(config)# end
Rodziejwicz-Bejnarowicz# show vlan
Use "show switch vlan" to view the vlans that have been assigned to Layer 2 switch ports.
Rodziejwicz-Bejnarowicz# show switch vlan
VLAN Name                Status    Ports
-----
1    inside                up        Et0/1, Et0/2, Et0/3, Et0/4
2    outside                up        Et0/5, Et0/6, Et0/7
Rodziejwicz-Bejnarowicz#
```

Z uwagi na taką konfigurację VLANów sieć laboratoryjna została podłączona do portu **e0/0**, a nasze komputery **e0/1** i **e0/2**.

DHCP na zaporze nie jest domyślnie aktywowane, nasze komputery dostały adres od serwera DHCP w pracowni.

```
Rodziejwicz-Bejnarowicz(config)# show dhcp
ERROR: % Incomplete command
Rodziejwicz-Bejnarowicz(config)# show dhcpd
ERROR: % Incomplete command
Rodziejwicz-Bejnarowicz(config)#
Rodziejwicz-Bejnarowicz(config)# show dhcpd
Rodziejwicz-Bejnarowicz(config)# show dhcpd
Rodziejwicz-Bejnarowicz(config)# show dhcpd ?

exec mode commands/options:
  binding      Show dhcp bindings
  state        Show dhcpd state
  statistics    Show dhcpd statistics
Rodziejwicz-Bejnarowicz(config)# show dhcpd state
Not Configured for DHCP
Rodziejwicz-Bejnarowicz(config)# show dhcpd b
Rodziejwicz-Bejnarowicz(config)# show dhcpd binding
Rodziejwicz-Bejnarowicz(config)#
```

Powyższe screenshotsy pokazują, że zmieniliśmy nazwę naszej zapory na nasze nazwiska.

Aby jednak nasze komputery otrzymały adres i zaczęło działać nam połączenie internetowe wymagane było zrestartowanie karty sieciowej w Windowsie (znalezienie tego zabrało nam cały pozostały czas po tym jak zresetowaliśmy naszą zaporę, co uniemożliwiło nam wykonanie ćwiczenia).


Po restarcie karty sieciowej działało nam połączenie internetowe, serwer DNS (`nslookup`), nie działał `ping` , ani `tracert` .

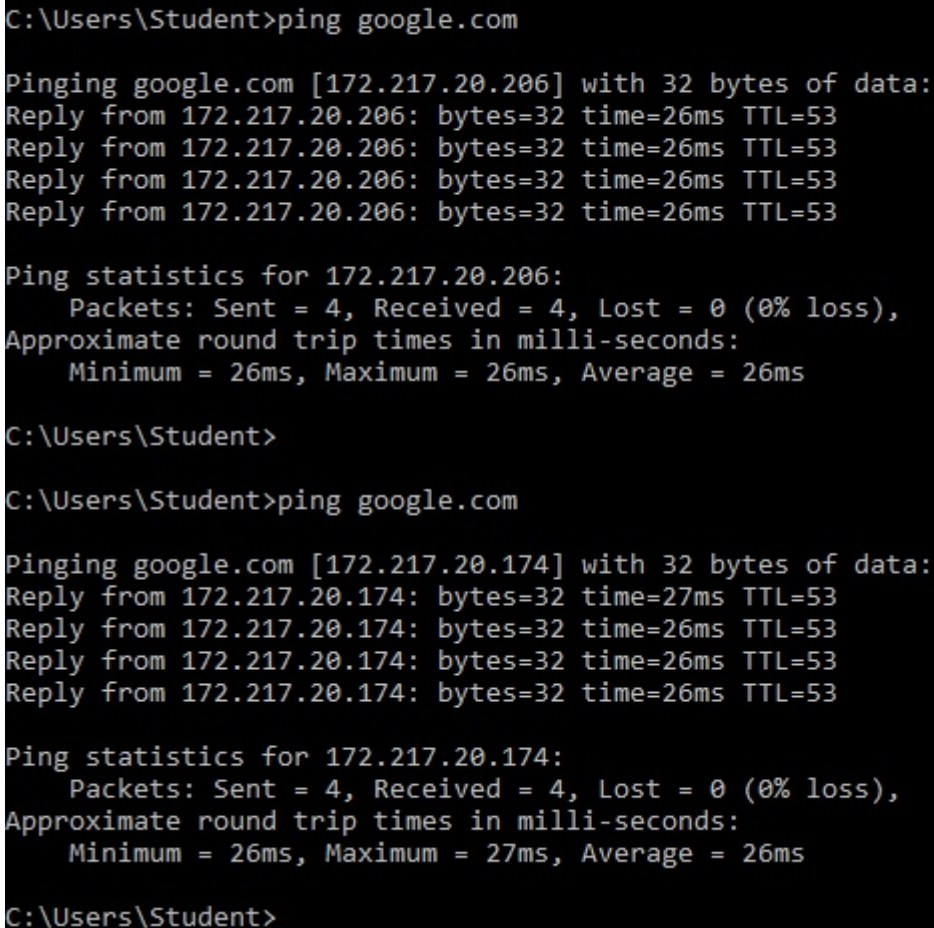
`ping` i `tracert` nie działał, ponieważ zaporą domyślnie blokuje powracające odpowiedzi `ICMP` .

Działanie pingów aktywowaliśmy za pomocą komend:

```
(config)# policy-map global_policy
(config-pmap)# class inspection_default
(config-pmap-c)# inspect icmp
```

Pingi działały, jednak `tracert` zachowywał się dziwnie.

 **Command Prompt**



```
C:\Users\Student>ping google.com

Pinging google.com [172.217.20.206] with 32 bytes of data:
Reply from 172.217.20.206: bytes=32 time=26ms TTL=53
Reply from 172.217.20.206: bytes=32 time=26ms TTL=53
Reply from 172.217.20.206: bytes=32 time=26ms TTL=53
Reply from 172.217.20.206: bytes=32 time=26ms TTL=53

Ping statistics for 172.217.20.206:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 26ms, Maximum = 26ms, Average = 26ms

C:\Users\Student>

C:\Users\Student>ping google.com

Pinging google.com [172.217.20.174] with 32 bytes of data:
Reply from 172.217.20.174: bytes=32 time=27ms TTL=53
Reply from 172.217.20.174: bytes=32 time=26ms TTL=53
Reply from 172.217.20.174: bytes=32 time=26ms TTL=53
Reply from 172.217.20.174: bytes=32 time=26ms TTL=53

Ping statistics for 172.217.20.174:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 26ms, Maximum = 27ms, Average = 26ms

C:\Users\Student>
```

Blokadę e-portalu i połączeń FTP uzyskaliśmy za pomocą listy ACL:

```
access-list acl_out; 3 elements; name hash: 0x4af10e18
access-list acl_out line 1 extended deny tcp any host 156.17.70.219 (hitcnt=0) 0x330d2669
access-list acl_out line 2 extended deny tcp any any eq ftp (hitcnt=0) 0x4b6342a3
access-list acl_out line 3 extended permit ip any any (hitcnt=0) 0xd85c9d2a
```

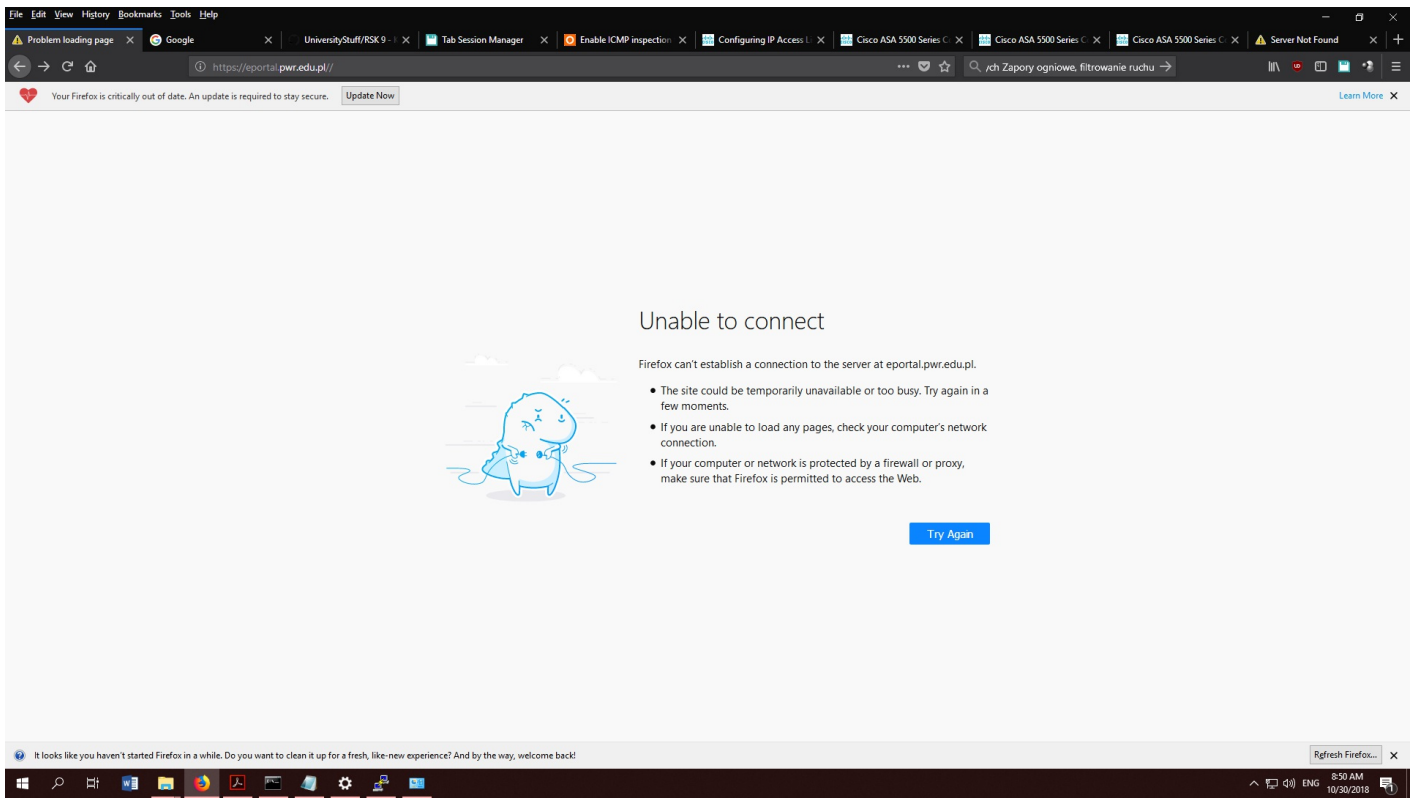
Stworzyliśmy ją następująco:

```
(config)# access-list acl_out extended deny tcp any host 156.17.70.219
(config)# access-list acl_out extended deny tcp any any eq ftp
(config)# access-list acl_out extended permit ip any any
```

Żałowana została przez nas na interfejs `Vlan2` , czyli `outside` w kierunku wyjściowym za pomocą komendy:

```
(config)# access-group acl_out out interface outside
```

Działanie blokady pokazuje poniższy screenshot (inne karty z innymi stronami są załadowane):



Działanie listy ACL zostało zgłoszone prowadzącemu.

Kolejnych punktów instrukcji nie udało nam się zrealizować z powodu zhamowania czasu na wcześniej wspomniane problemy.