Wrocław, 02.12.2020

Bezpieczeństwo sieci komputerowych

Laboratorium 4

Zapory ogniowe, filtrowanie ruchu (Cisco ASA)

Prowadzący: dr inż. Marcin Markowski

Autorka: Agnieszka Płoszaj 218353

Zadanie zostało wykonane przy wykorzystaniu komputera z systemem windows 10 i programu *Cisco Packet Tracer 7.3.1*.

Zadanie 1

Na początek połączono się z ASA za pomocą konsoli. Następnie została wyświetlona bieżąca konfiguracja IP interfejsów sieciowych, przy pomocy polecenia:
`show int ip brief`
(ilustracja 1).
Przy pomocy poleceń
`show ip address` oraz
`show switch vlan`
zostały wyświetlone szczegóły VLAN i adresacji IP (ilustracja 2). Porty Et0/1, Et0/2, Et0/3, Et0/4, Et0/5, Et0/6 oraz Et0/7 domyślnie są przypisane do VLAN 1. Port Et0/0 jest domyślnie przypisany do VLAN 2.
Następnie przy pomocy polecenia
`hostname Ploszaj`
została zmieniona nazwa urządzenia.

```
ciscoasa#show int ip brief
Interface              IP-Address      OK? Method Status                Protocol

Ethernet0/0            unassigned      YES unset  down                  down

Ethernet0/1            unassigned      YES unset  down                  down

Ethernet0/2            unassigned      YES unset  down                  down

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

Vlan1                  192.168.1.1     YES CONFIG up                    down

Vlan2                  unassigned      YES DHCP   up                    down
```

Ilustracja 1 Bieżąca konfiguracja urządzenia

```
ciscoasa#show ip address
System IP Addresses:
Interface              Name                IP address      Subnet mask     Method
Vlan1                  inside              192.168.1.1     255.255.255.0   CONFIG
Vlan2                  outside             unassigned      unassigned      DHCP

Current IP Addresses:
Interface              Name                IP address      Subnet mask     Method
Vlan1                  inside              192.168.1.1     255.255.255.0   CONFIG
Vlan2                  outside             unassigned      unassigned      DHCP

ciscoasa#show switch vlan

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    inside                           down      Et0/1, Et0/2, Et0/3, Et0/4
                                                Et0/5, Et0/6, Et0/7
2    outside                          down      Et0/0
```

Ilustracja 2 Szczegóły VLAN oraz adresacji IP

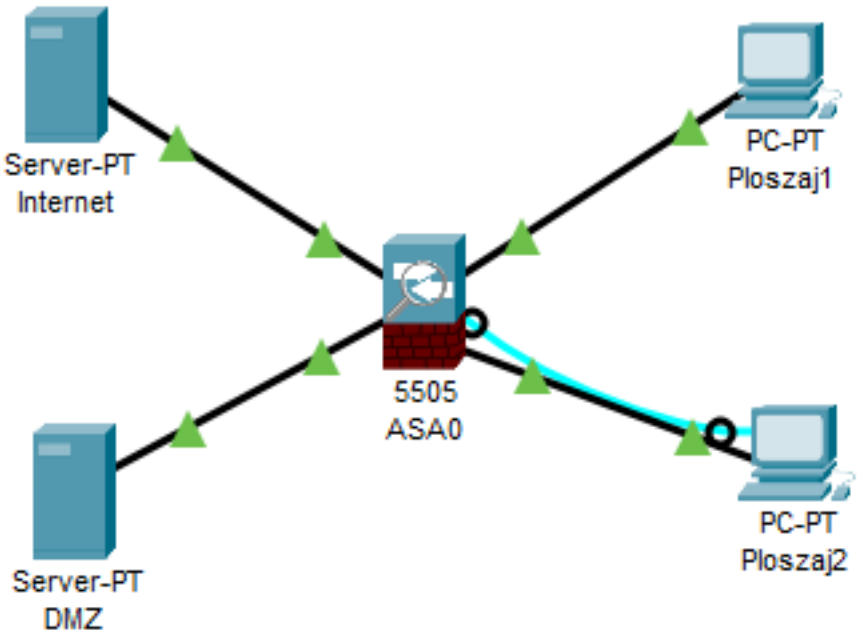
Zadanie 2

Zgodnie z rysunkiem z instrukcji została zbudowana sieć (ilustracja 3). Sieć internet została podłączona do odpowiedniego prekonfigurowanego portu zapory, którym jest port Et0/0. Na serwerze zostały uruchomione usługi HTTP, FTP, TFTP oraz DNS (ilustracja 4). Następnie zostały skonfigurowane interfejsy VLAN 1 oraz VLAN 2 (ilustracja 5 i 6). W następnej kolejności przy pomocy polecenia ping zostało sprawdzone połączenie z serwerem internetowym oraz drugim komputerem (ilustracja 7). Został też sprawdzony dostęp do usług na serwerze internetowym (ilustracja 8). Niestety nic nie działało. Dlatego, zostały wykonane dodatkowe polecenia, niezbędne do właściwego działania. W tym celu zostały wykonane polecenia:

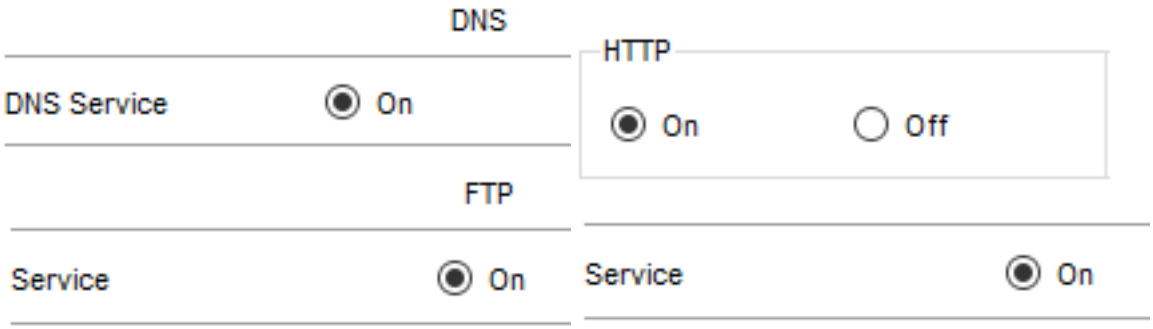
```
object network obj_any
subnet 0.0.0.0 0.0.0.0
nat (inside,outside) dynamic interface
class-map inspection_default
match default-inspection-traffic
policy-map global_policy
class inspection_default
inspect http
inspect ftp
inspect tftp
Inspect icmp
service-policy global_policy global
```

Przyczyną dla której zaczęło działać dopiero po wpisaniu wszystkich tych poleceń jest to, że w PT, ASA domyślnie nie zezwala na ruch pomiędzy sieciami zewnętrznymi i wewnętrznymi. Dodatkowo trzeba było zezwolić na konkretne rodzaje ruchu oraz protokoły. Wynik działania polecenia ping oraz dostęp do usług zostały pokazane na ilustracjach 9 i 10.

Następnie została podjęta próba utworzenia konta dla administratora, niestety okazało się to niemożliwe do zrealizowania (ilustracja 11).



Ilustracja 3 Schemat połączeń



Ilustracja 4 Uruchomienie usług

```
Ploszaj#conf t
Ploszaj(config)#interface vlan 1
Ploszaj(config-if)#nameif inside
Ploszaj(config-if)#route outside 0.0.0.0 0.0.0.0 192.168.111.111
Ploszaj(config)#interface vlan 1
Ploszaj(config-if)#dhcpd address 192.168.1.5-192.168.1.100 inside
Warning, DHCP pool range is limited to 32 addresses, set address range as: 192.168.1.5-192.168.1.36
Ploszaj(config)#interface vlan 1
Ploszaj(config-if)#dhcpd address 192.168.1.5-192.168.1.36 inside
Ploszaj(config)#interface vlan 1
Ploszaj(config-if)#dhcp enable inside
```

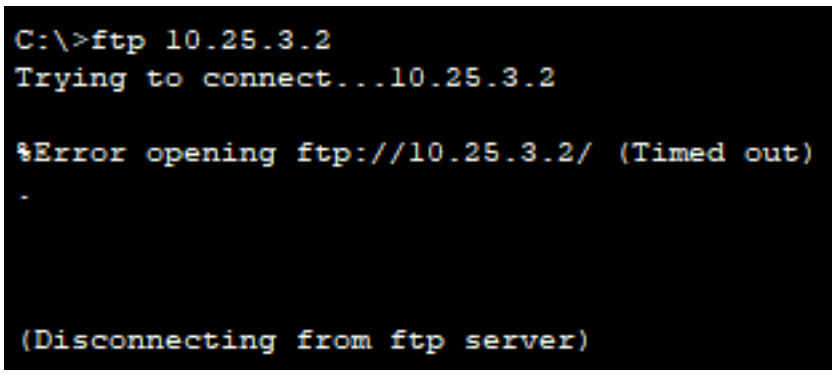
Ilustracja 5 Interfejs VLAN 1

```
Ploszaj(config)#interface VLAN 1
Ploszaj(config-if)#ex
Ploszaj(config)#dhcp address 192.168.1.5-192.168.1.100 inside
Warning, DHCP pool range is limited to 32 addresses, set address range as: 192.168.1.5-192.168.1.36
Ploszaj(config)#dhcp address 192.168.1.5-192.168.1.36 inside
Ploszaj(config)#dhcp enable inside
Ploszaj(config)#interface VLAN 2
Ploszaj(config-if)#ip address 10.25.3.0 255.255.255.0
Ploszaj(config-if)#no shutdown
Ploszaj(config-if)#ex
Ploszaj(config)#ex
Ploszaj#show int ip brief
Interface              IP-Address      OK? Method Status                Protocol

Ethernet0/0            unassigned      YES NVRAM  up                    up

Ethernet0/1            unassigned      YES NVRAM  up                    up

Ethernet0/2            unassigned      YES NVRAM  up                    up

Ethernet0/3            unassigned      YES NVRAM  down                  down

Ethernet0/4            unassigned      YES NVRAM  down                  down

Ethernet0/5            unassigned      YES NVRAM  down                  down

Ethernet0/6            unassigned      YES NVRAM  down                  down

Ethernet0/7            unassigned      YES NVRAM  up                    up

Vlan1                  192.168.1.1     YES manual up                    up

Vlan2                  10.25.3.0       YES manual up                    up
```

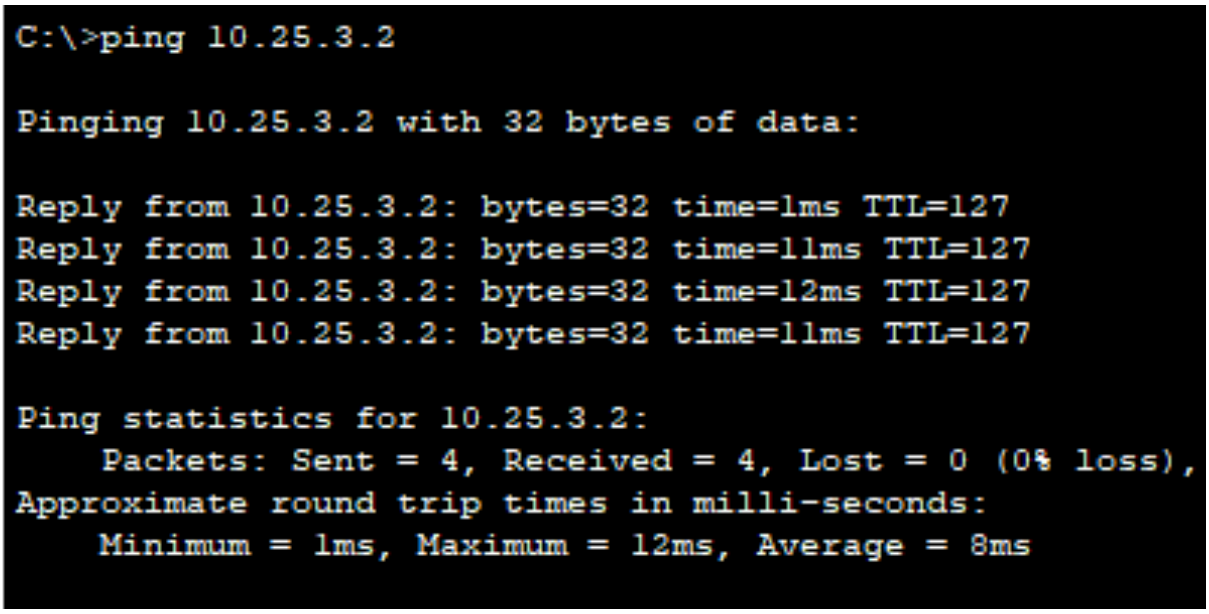
Ilustracja 6 Interfejsy VLAN 1 i VLAN 2

```
Packet Tracer PC Command Line 1.0
C:\>ping 192.168.1.5

Pinging 192.168.1.5 with 32 bytes of data:

Reply from 192.168.1.5: bytes=32 time=1ms TTL=128
Reply from 192.168.1.5: bytes=32 time=1ms TTL=128
Reply from 192.168.1.5: bytes=32 time<1ms TTL=128
Reply from 192.168.1.5: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.1.5:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>ping 10.25.3.0

Pinging 10.25.3.0 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 10.25.3.0:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

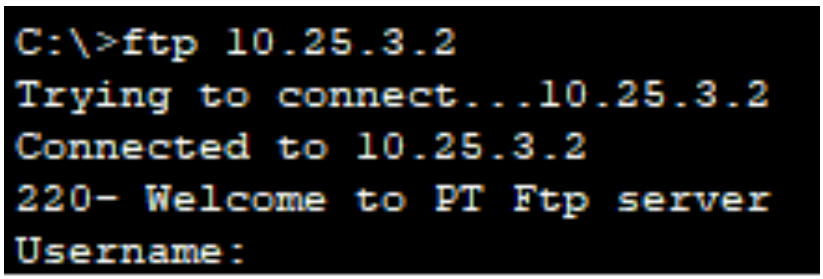
Ilustracja 7 ping –nieudane połączenie



Ilustracja 8 FTP – nieudane połączenie



Ilustracja 9 ping – udane połączenie



Ilustracja 10 FTP – udane połączenie

```
Ploszaj(config)#username PloszajAgnieszka password ploszaj ?

configure mode commands/options:
  encrypted  Indicates the <password> entered is encrypted
  <cr>
Ploszaj(config)#username PloszajAgnieszka password ploszaj privilege 15
                                                          ^
% Invalid input detected at '^' marker.
```

Ilustracja 11 Tworzenie konta administratora

Zadanie 3

Pierwsza z reguł została zrealizowana w zadaniu 2 poprzez zmiany dokonywane w obiekcie *policy-map*.
Druga reguła (blokująca protokół ftp z sieci LAN) została uzyskana poprzez polecenie:
access-list ftp_block deny tcp any any eq 21.
Jednak, żeby nie blokować całego ruchu internetowego zostało użyte drugie polecenie:
access-list ftp_block permit ip any any
access-group ftp_block in interface inside
(ilustracja 12). Następnie przy pomocy polecenia
show access-list
została wyświetlona lista ACL (ilustracja 13). Zostało również sprawdzone działanie powyższych reguł (ilustracja 9 i 14).

```
Ploszaj(config)#access-list ftp_block deny tcp any any ?

configure mode commands/options:
  eq     Match only packets on a given port number
  gt     Match only packets with a greater port number
  lt     Match only packets with a lower port number
  neq    Match only packets not on a given port number
  range  Match only packets in the range of port numbers
  <cr>
Ploszaj(config)#access-list ftp_block deny tcp any any eq
% Incomplete command.
Ploszaj(config)#access-list ftp_block deny tcp any any eq ?

configure mode commands/options:
  <0-65535>  Port number
  domain     Domain Name Service (DNS, 53)
  ftp        File Transfer Protocol (21)
  pop3       Post Office Protocol v3 (110)
  smtp       Simple Mail Transport Protocol (25)
  telnet     Telnet (23)
  www        World Wide Web (HTTP, 80)
Ploszaj(config)#access-list ftp_block deny tcp any any eq 21
```

Ilustracja 12 Dodanie reguły do ACL

```
Ploszaj#show access-list
access-list cached ACL log flows: total 0, denied 0 (deny-flow-max 4096) alert-interval 300
access-list ftp_block; 2 elements; name hash: 0x69268e27
access-list ftp_block line 1 extended deny tcp any any eq ftp(hitcnt=24) 0xe2273eb9
access-list ftp_block line 2 extended permit ip any any(hitcnt=0) 0x1e3ee453
```

Ilustracja 13 Lista ACL

```
C:\>ftp 10.25.3.2
Trying to connect...10.25.3.2

%Error opening ftp://10.25.3.2/ (Timed out)
.



(Disconnecting from ftp server)
```

Ilustracja 14 Blokowane FTP

Zadanie 4

Następnie została skonfigurowana strefa DMZ (ilustracja 15).

```
Ploszaj(config)#object network strefa_dmz
Ploszaj(config-network-object)#host 172.16.3.5
Ploszaj(config-network-object)#nat(dmz,outside) static 192.168.0.143
                               ^
% Invalid input detected at '^' marker.

Ploszaj(config-network-object)#nat (dmz,outside) static 192.168.0.143
Ploszaj(config-network-object)#end
```

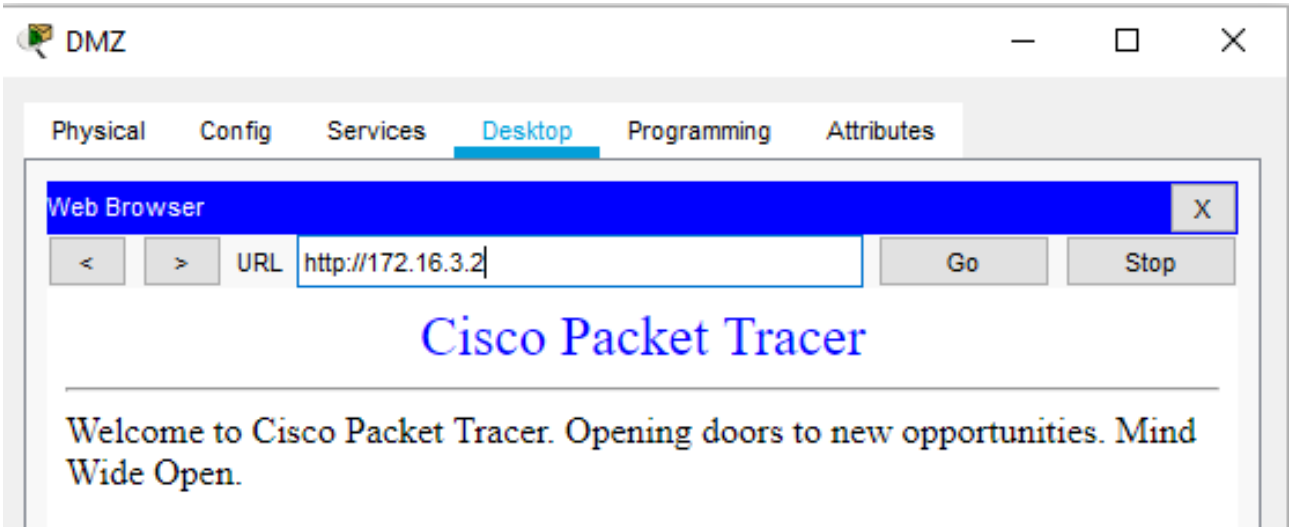
Ilustracja 15 Strefa DMZ

W następnej kolejności została usunięta reguła z zadania 3 (ilustracja 16).

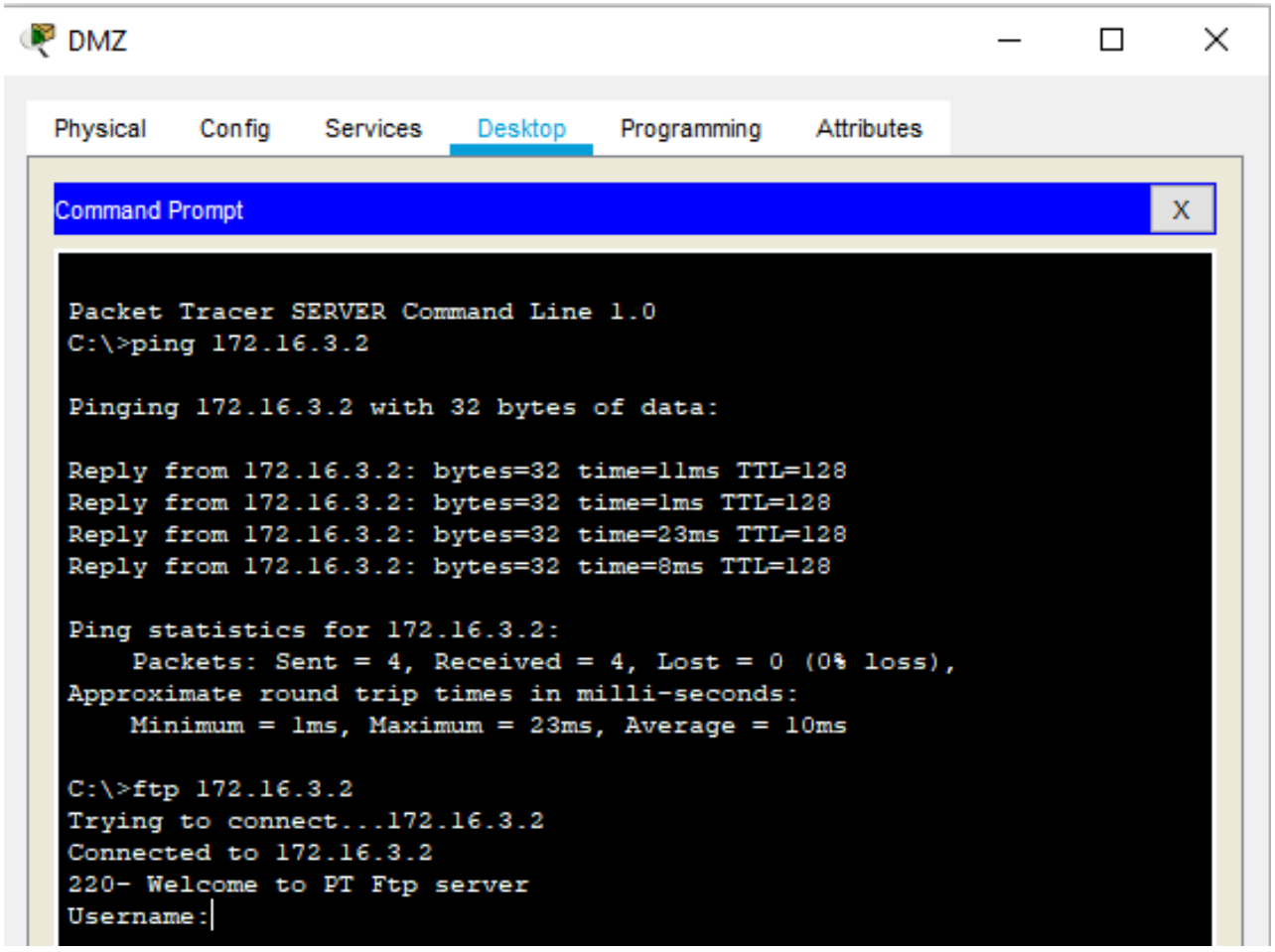
```
Ploszaj(config)#no access-list ftp_block extended deny tcp any any eq ftp
Ploszaj(config)#no access-list ftp_block extended permit ip any any
```

Ilustracja 16 Usunięcie reguły z zadania 3

Następnie na serwerze DMZ zostały uruchomione usługi HTTP, FTP oraz odpowiadanie na ping. Wynik działania widać na ilustracjach 17 i 18.



Ilustracja 17 DMZ – działanie HTTP



Ilustracja 18 DMZ – działanie ping oraz FTP

Ostatnie zadanie polegało na konfiguracji reguł dostępu do serwera w DMZ (dostęp z zewnątrz dla ping oraz FTP). W tym celu zostały użyte poniższe polecenia:
access-list acl_dmz permit icmp any host 172.16.3.2 eq 21
access-group acl_dmz in interface outside
(ilustracja 19).
Następnie została wykonana weryfikacja działania reguł. Na początek zostało wykorzystane polecenie
show access-list
(ilustracja 20). Następnie, przy pomocy konsoli została sprawdzona łączność od strony Internetu (ilustracja 21). Jak widać na załączonych poniżej ilustracjach udało się poprawnie skonfigurować serwer w DMZ.

```
Ploszaj(config)#access-list acl_dmz permit tcp any host 172.16.3.2 eq 21
```

Ilustracja 19 DMZ – lista ACL

```
Ploszaj(config)#show access-list
access-list cached ACL log flows: total 0, denied 0 (deny-flow-max 4096) alert-interval 300
access-list acl_dmz; 2 elements; name hash: 0xaldd5a37
access-list acl_dmz line 1 extended permit icmp any host 172.16.3.2(hitcnt=0) 0x304ec463
access-list acl_dmz line 2 extended permit tcp any host 172.16.3.2 eq ftp(hitcnt=0) 0x56c77cb8
```

Ilustracja 20 DMZ – polecenie show access-list

```
C:\>ftp 172.16.3.2
Trying to connect...172.16.3.2
Connected to 172.16.3.2
220- Welcome to PT Ftp server
Username:
```

Ilustracja 21 DMZ – udane połączenie