

Laboratorium 8 – Podstawowa konfiguracja sprzętowej zapory sieciowej ASA 5505

Cele ćwiczenia

Celem ćwiczenia jest nabycie umiejętności konfigurowania podstawowych ustawień oraz funkcjonalności zapory sieciowej ASA 5505. Cele szczegółowe są następujące:

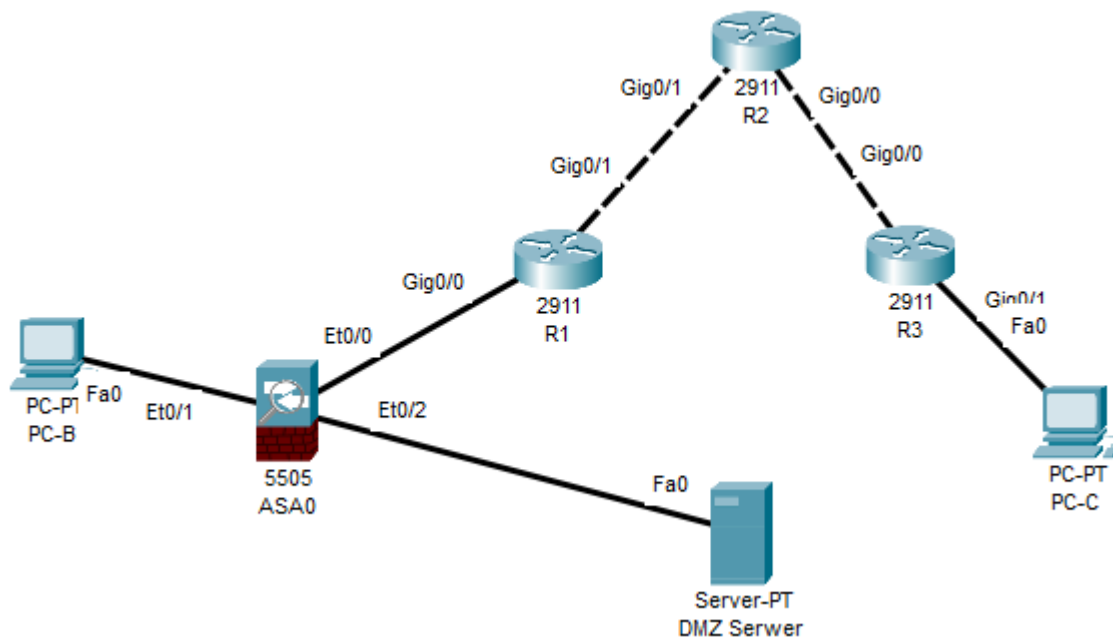
1. Konfiguracja sieci ze sprzętową zaporą sieciową ASA 5505
2. Dostęp do konsoli ASA i używanie trybu konfiguracji CLI do konfiguracji podstawowych ustawień
3. Konfiguracja podstawowych ustawień ASA i poziomów bezpieczeństwa interfejsu
4. Konfiguracja routingu, translacji adresów i polityki inspekcji
5. Konfiguracja DHCP, AAA i SSH
6. Konfiguracja DMZ, statycznego NAT i list ACL

Opis topologii logicznej i fizycznej sieci

1. Komputer PC-B o adresie IP 192.168.1.3/24 połączony łączem FastEthernet0 z portem Ethernet0/1 ASA 5505, który należy do VLAN1 o adresie 192.168.1.1/24.
2. Serwer DMZ o adresie IP 192.168.2.3/24 połączony łączem FastEthernet0 z portem Ethernet 0/2 ASA 5505, który należy do VLAN3 o adresie 192.168.2.1/24.
3. Port Ethernet 0/0 ASA, który należy do VLAN2 o adresie 209.165.200.226/29, połączony z portem Gigabit Ethernet 0/0 rutera R1 o adresie 209.165.200.225/29.
4. Port Gigabit Ethernet 0/1 o adresie 10.1.1.1/30 rutera R1 połączony z portem Gigabit Ethernet 0/1 rutera R2 o adresie 10.1.1.2/30.
5. Port Gigabit Ethernet 0/0 rutera R2 o adresie 10.2.2.1/30 połączony z portem Gigabit Ethernet 0/0 rutera R3 o adresie 10.2.2.2/30.

6. Komputer PC-C o adresie 172.16.3.3 połączony z portem Gigabit Ethernet 0/1 rutera R3 o adresie 172.16.3.1/24.

Graficzną reprezentację opisaną topologię przedstawiono na poniższym rysunku.



Przebieg ćwiczenia

Połączenie urządzeń zgodnie z topologią przedstawioną w poprzednim rozdziale

Nadanie adresów IP urządzeniom końcowym

1. Komputer PC-B

Adres 192.168.1.3 z maską 24 bitową, brama domyślna 192.168.1.1/24

2. Komputer PC-C

Adres 192.168.3.3 z maską 24 bitową, brama domyślna 192.168.3.1/24

3. Serwer DMZ

Adres 192.168.2.3 z maską 24 bitową, brama domyślna 192.168.2.1/24

Nadanie adresów IP poszczególnym interfejsom ruterów R1, R2, R3.

```
R1(config)# interface g0/0
R1(config-if)# ip address 209.165.200.225 255.255.255.248
R1(config-if)# no shutdown
R1(config)# interface g0/1
R1(config-if)# ip address 10.1.1.1 255.255.255.252
R1(config-if)# no shutdown
```

Wykonaj te same czynności na ruterach R2 i R3.

Konfiguracja protokołu OSPF na ruterach R1, R2, R3 (nr procesu 1)

```
R1(config)# router ospf 1
R1(config-if)# network 209.165.200.224 0.0.0.7 area 0
R1(config-if)# network 10.1.1.0 0.0.0.3 area 0
```

Wykonaj te same czynności związane z konfiguracją protokołu OSPF na ruterach R2 i R3.

Uzyskanie dostępu do linii konsoli urządzenia ASA i skonfigurowanie podstawowych ustawień korzystając z linii poleceń

Określenie wersji urządzenia, dostępnych interfejsów i licencji oprogramowania

ASA 5505 jest wyposażony w zintegrowany ośmioportowy przełącznik Ethernet. Porty od E0/0 do E0/5 to normalne porty Fast Ethernet, a porty E0/6 i E0/7 to porty PoE (power over Ethernet) do użytku z urządzeniami PoE, takimi jak telefony IP lub kamery sieciowe.

Użyj polecenia **show version**, aby pozyskać podstawowe informacje o urządzeniu i jego parametrach

```
ciscoasa> enable
Password: class (or press Enter if none set)
ciscoasa# show version
Cisco Adaptive Security Appliance Software Version 8.4(2)
Device Manager Version 6.4(5)

Compiled on Wed 15-Jun-11 18:17 by mnguyen
```



System image file is "disk0:/asa842-k8.bin

Config file at boot was "startup-config"

ciscoasa up 20 minutes 40 seconds

Hardware: ASA5505, 512 MB RAM, CPU Geode 500 MHz

Internal ATA Compact Flash, 128MB

BIOS Flash M50FW016 @ 0xffff00000, 2048KB

Encryption hardware device : Cisco ASA-5505 on-board accelerator
(revision 0x0)

BOOT-2.00 Boot microcode : CN1000-MC-

SSLm-PLUS-2.03 SSL/IKE microcode : CNLite-MC-

IPSECm-MAIN-2.06 IPSec microcode : CNlite-MC-

Number of accelerators: 1

0: Int: Internal-Data0/0	: address is 44d3.caef.1e22, irq 11
1: Ext: Ethernet0/0	: address is 000A.4175.2001, irq 255
2: Ext: Ethernet0/1	: address is 000A.4175.2002, irq 255
3: Ext: Ethernet0/2	: address is 000A.4175.2003, irq 255
4: Ext: Ethernet0/3	: address is 000A.4175.2004, irq 255
5: Ext: Ethernet0/4	: address is 000A.4175.2005, irq 255
6: Ext: Ethernet0/5	: address is 000A.4175.2006, irq 255
7: Ext: Ethernet0/6	: address is 000A.4175.2007, irq 255
8: Ext: Ethernet0/7	: address is 000A.4175.2008, irq 255
9: Int: Internal-Data0/1	: address is 0000.0003.0002, irq 255
10: Int: Not used	: irq 255
11: Int: Not used	: irq 255

Licensed features for this platform:

Maximum Physical Interfaces	: 8	perpetual
VLANs	: 3	DMZ Restricted
Dual ISPs	: Disabled	perpetual
VLAN Trunk Ports	: 0	perpetual
Inside Hosts	: 10	perpetual
Failover	: Disabled	perpetual
VPN-DES	: Enabled	perpetual
VPN-3DES-AES	: Enabled	perpetual
AnyConnect Premium Peers	: 2	perpetual
AnyConnect Essentials	: Disabled	perpetual
Other VPN Peers	: 10	perpetual
Total VPN Peers	: 25	perpetual
Shared License	: Disabled	perpetual
AnyConnect for Mobile	: Disabled	perpetual
AnyConnect for Cisco VPN Phone	: Disabled	perpetual
Advanced Endpoint Assessment	: Disabled	perpetual
UC Phone Proxy Sessions	: 2	perpetual
Total UC Proxy Sessions	: 2	perpetual
Botnet Traffic Filter	: Disabled	perpetual
Intercompany Media Engine	: Disabled	perpetual

This platform has a Base license.

Serial Number: JMX15368J8T-

Running Permanent Activation Key: 0xCBA5B7A8 0x2A9AEC0C 0xCA672059
0xA5838891 0xC345BDD3

Configuration register is 0x1

Configuration has not been modified since last system restart.

Sprawdzenie systemu plików i zawartości pamięci flash

W celu wyświetlenia systemu plików urządzenia ASA, skorzystaj z polecenia **show file system**. Sprawdź, jakie prefiksy są obsługiwane.

```
ciscoasa# show file system
```



File Systems:

	Size (b)	Free (b)	Type	Flags	Prefixes
*	128573440	123001856	disk	rw	disk0: flash:

Wyświetl zawartość pamięci flash, korzystając z polecenia **show flash**.

```
ciscoasa# show flash
--#--  --length--  -----date/time-----  path
1    5571584                               asa842-k8.bin
```

```
128573440 bytes total (123001856 bytes free)
```

Wyświetlenie bieżącej konfiguracji urządzenia

Wyświetl bieżącą konfigurację, posługując się poleceniem **show running-config**.

```
ciscoasa# show running-config
: Saved
:
ASA Version 8.4(2)
!
hostname ciscoasa
names
!
interface Ethernet0/0
  switchport access vlan 2
!
interface Ethernet0/1
!
interface Ethernet0/2
!
interface Ethernet0/3
!
interface Ethernet0/4
!
```



```
interface Ethernet0/5
!
interface Ethernet0/6
!
interface Ethernet0/7
!
interface Vlan1
  nameif inside
  security-level 100
  ip address 192.168.1.1 255.255.255.0
!
interface Vlan2
  nameif outside
  security-level 0
  ip address dhcp
!
!
telnet timeout 5
ssh timeout 5
!
dhcpd auto_config outside
!
!
dhcpd address 192.168.1.5-192.168.1.36 inside
dhcpd enable inside
!
```

W przypadku konieczności przywrócenia ustawień fabrycznych, należy wydać polecenie **configure factory-default**.

```
ciscoasa(config)# configure factory-default
```

Usuwanie istniejącej konfiguracji urządzenia ASA.

W celu usunięcia konfiguracji urządzenia, przechowywanej w pliku startup-config w pamięci flash, należy wydać polecenie **write erase**.

```
ciscoasa# write erase
```

Następnie, należy wydać polecenie **reload**, które spowoduje restart urządzenia. Urządzenie uruchomi się bez wcześniejszych ustawień. W przypadku, gdy po wydaniu polecenia reload pojawi się ostrzeżenie, że konfiguracja została zmieniona i pytanie, czy zapisać bieżącą konfigurację, należy odpowiedzieć „no” i kontynuować restart urządzenia.

```
ciscoasa# reload
```

Konfiguracja podstawowych ustawień i interfejsów ASA

Konfiguracja nazwy urządzenia i nazwy domeny.

Wejść do trybu konfiguracji ogólnej:

```
ciscoasa# config t
```

```
ciscoasa(config)#
```

Skonfiguruj nazwę własną ASA:

```
ciscoasa(config)# hostname ASA-CS
```

Skonfiguruj domenę:

```
ASA-CS(config)# domain-name ioc.com
```

Konfiguracja dostępu do urządzenia.

Ustaw hasło dostępu do urządzenia. Domyślnym hasłem jest cisco. Należy je zmienić przy pierwszym uruchomieniu, posługując się poleceniem **passwd** lub **password**:

```
ASA-CS(config)# passwd cisco
```

Ustaw hasło wymagane do dostępu uprzywilejowanego (tryb „privileged EXEC”), korzystając z polecenia **enable password**:

```
ASA-CS(config)# enable password class
```


Ustawianie daty i czasu.

Poprawną wartość daty i czasu można ustawić ręcznie korzystając z polecenia **clock set** (zalecany rozwiązaniem w sieciach produkcyjnych jest korzystanie z protokołu NTP):

```
ASA-CS (config) # clock set 22:22:00 april 22 2022
```

Konfiguracja interfejsów wewnętrznych i zewnętrznych.

Skonfiguruj logiczny interfejs VLAN 1 dla sieci wewnętrznej (192.168.1.0/24) i ustaw najwyższy poziom bezpieczeństwa na 100:

```
ASA-CS (config) # interface vlan 1
ASA-CS (config-if) # nameif inside
ASA-CS (config-if) # ip address 192.168.1.1 255.255.255.0
ASA-CS (config-if) # security-level 100
```

Utwórz logiczny interfejs VLAN 2 dla sieci zewnętrznej (209.165.200.224/29) i ustaw poziom zabezpieczeń na najniższe ustawienie 0 i uzyskaj dostęp do interfejsu VLAN 2:

```
ASA-CS (config-if) # interface vlan 2
ASA-CS (config-if) # nameif outside
ASA-CS (config-if) # ip address 209.165.200.226 255.255.255.248
ASA-CS (config-if) # no shutdown
```

Użyj polecenia **show interface ip brief**, aby upewnić się, że porty ASA Layer 2 E0/0 (dla VLAN 2) i E0/1 (dla VLAN 1) są aktywne:

```
ASA-CS (config-if) # show interface ip brief
```

Interface Protocol	IP-Address	OK?	Method	Status
Ethernet0/0 up	unassigned	YES	unset	up
Ethernet0/1 up	unassigned	YES	unset	up
Ethernet0/2 up	unassigned	YES	unset	up



Ethernet0/3 down	unassigned	YES	unset	down
Ethernet0/4 down	unassigned	YES	unset	down
Ethernet0/5 down	unassigned	YES	unset	down
Ethernet0/6 down	unassigned	YES	unset	down
Ethernet0/7 down	unassigned	YES	unset	down
Vlan1 up	192.168.1.1	YES	CONFIG	up
Vlan2 up	209.165.200.226	YES	manual	up

Przypisz port E0/1 do sieci VLAN 1, a port E0/0 do sieci VLAN 2:

```
ASA-CS(config)# interface e0/1
ASA-CS(config-if)# switchport access vlan 1
ASA-CS(config-if)# interface e0/0
ASA-CS(config-if)# switchport access vlan 2
```

Wyświetl informacje dotyczące interfejsów VLAN:

```
ASA-CS# 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                209.165.200.226
255.255.255.248 manual
```

Current IP Addresses:

Interface Method	Name	IP address	Subnet mask
Vlan1 255.255.255.0	inside CONFIG	192.168.1.1	
Vlan2 255.255.255.248	outside manual	209.165.200.226	

Użyj polecenia **show switch vlan**, aby wyświetlić wewnętrzne i zewnętrzne sieci VLAN skonfigurowane w ASA oraz wyświetlić przypisane do nich porty:

```
ASA-CS# show switch vlan
```

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

Przetestuj łączność z ASA.

Powinieneś być w stanie otrzymać odpowiedź na wysyłane pakiety ICMP Echo Request (ping) z PC-B na wewnętrzny adres interfejsu. W przypadku problemów, sprawdź konfigurację interfejsów i adresów IP:

```
ASA-CS# ping 192.168.1.3
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.3, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
```

Z komputera PC-C wyślij ping do interfejsu VLAN 2 (zewnętrznego), tj. na adres IP 209.165.200.226.

Próba powinna zakończyć się niepowodzeniem.

Konfigurowanie routingu, translacji adresów i polityki inspekcji

Konfiguracja statycznej trasy domyślnej na urządzeniu ASA

Utwórz domyślną trasę (same zera w części sieci i maski) za pomocą polecenia **route**, skojarz ją z zewnętrznym interfejsem ASA i wskaż jako ruter następnego skoku interfejs G0/0 rutera R1, dostępnego pod adresem IP 209.165.200.225, który będzie pełnić funkcję bramy ostatniej szansy:

```
ASA-CS (config) # route outside 0.0.0.0 0.0.0.0 209.165.200.225
```

Wyдай polecenie **show route**, aby wyświetlić tablicę routingu ASA w celu sprawdzenia, czy dodana została trasa statyczna, utworzona w poprzednim kroku:

```
ASA-CS# show route
```

```
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
```

```
        D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
        N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
        E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
        i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS
inter area
        * - candidate default, U - per-user static route, o - ODR
        P - periodic downloaded static route
```

```
Gateway of last resort is 209.165.200.225 to network 0.0.0.0
```

```
C      192.168.1.0 255.255.255.0 is directly connected, inside, Vlan1
      209.165.200.0/29 is subnetted, 2 subnets
```

```
C          209.165.200.0 255.255.255.248 is directly connected, outside,
Vlan2
```

```
C          209.165.200.224 255.255.255.248 is directly connected,
outside, Vlan2
```

```
S*      0.0.0.0/0 [1/0] via 209.165.200.225
```

Sprawdź łączność między ASA i R1:

```
ASA-CS# ping 10.1.1.1
```

```
Type escape sequence to abort.
```



```
Sending 5, 100-byte ICMP Echos to 10.1.1.1, timeout is 2 seconds:
```

```
!!!!!
```

```
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/0 ms
```

Konfiguracja translacji adresów PAT z wykorzystaniem obiektów sieciowych.

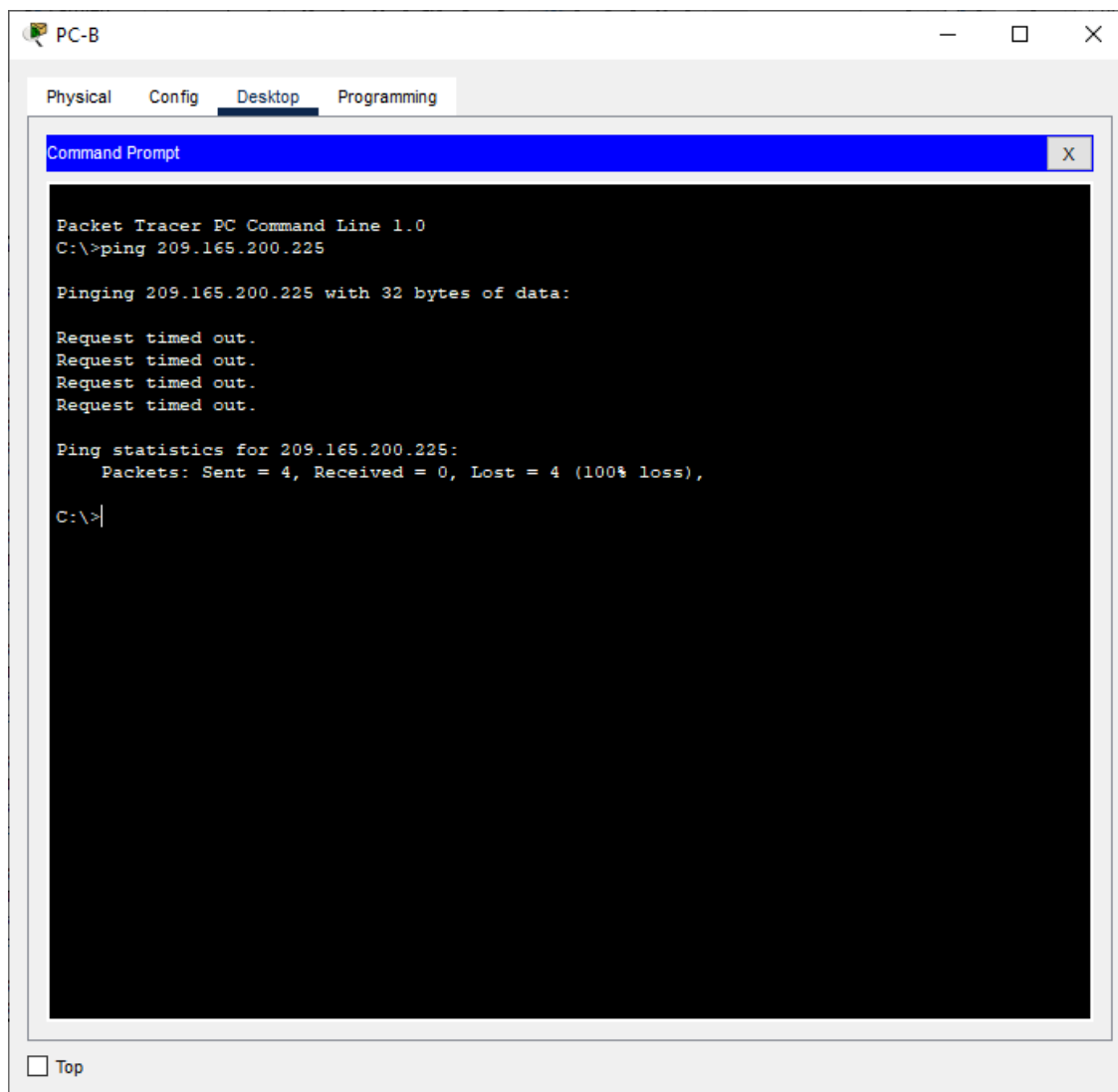
Utwórz obiekt sieciowy INSIDE-NET i przypisz mu atrybuty za pomocą poleceń **subnet** i **nat**:

```
ASA-CS(config)# object network INSIDE-NET  
ASA-CS(config-network-object)# subnet 192.168.1.0 255.255.255.0  
ASA-CS(config-network-object)# nat (inside,outside) dynamic  
interface
```

Skorzystaj z polecenia **show nat**, aby sprawdzić liczbę przeprowadzonych translacji:

```
ASA-CS# show nat  
Auto NAT Policies (Section 2)  
1 (inside) to (outside) source dynamic INSIDE-NET interface  
translate_hits = 0, untranslate_hits = 0
```

Z komputera PC-B spróbuj spingować interfejs R1 pod adresem IP 209.165.200.225:



Wydaj ponownie polecenie **show nat** na ASA. Zauważ, że spośród „pingów” z PC-B cztery zostały przetłumaczone, a trzy nie, ponieważ ICMP nie jest nadzorowany przez globalną politykę inspekcji. Wychodzące wiadomości Echo Request zostały przetłumaczone, a powracające odpowiedzi Echo Replies zostały zablokowane przez zasady zapory.

```
ASA-CS# show nat
Auto NAT Policies (Section 2)
1 (inside) to (outside) source dynamic INSIDE-NET interface
  translate_hits = 4, untranslate_hits = 3
```

Wykonaj ponownie polecenie ping z PC-B do R1 i postaraj się jak najszybciej wydać polecenie **show xlate**, aby zobaczyć tłumaczenie adresów:



```
ASA-CS# show xlate
1 in use, 1 most used
Flags: D - DNS, e - extended, I - identity, i - dynamic, r -
portmap, s - static, T - twice, N - net-to-net
ICMP PAT from inside:192.168.1.3/3 to
outside:209.165.200.226/57645 flags i idle 00:00:27, timeout
0:00:30
```

Modyfikacja globalnej polityki inspekcji MPF

Utwórz domyślną „class-map”:

```
ASA-CS (config)# class-map inspection_default
ASA-CS (config-cmap)# match default-inspection-traffic
```

Dodaj inspekcję ruchu ICMP do listy map polityk:

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

Włącz globalną mapę zasad

```
ASA-CS (config)# service-policy global_policy global
```

Wyświetl domyślną mapę zasad MPF, aby sprawdzić, czy ICMP jest teraz wymieniony w regułach inspekcji.

```
ASA-CS# show run policy-map
policy-map global_policy
  class inspection_default
    inspect icmp
```

Z PC-B spróbuj pingować R1 pod adresem IP 209.165.200.225. Tym razem pingi powinny zakończyć się powodzeniem, ponieważ ruch ICMP jest teraz sprawdzany, a ruch powrotny jest zgodny z zasadami:



```
PC-B
Physical Config Desktop Programming
Command Prompt
Pinging 209.165.200.225 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 209.165.200.225:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>ping 209.165.200.225

Pinging 209.165.200.225 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 209.165.200.225:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>ping 209.165.200.225

Pinging 209.165.200.225 with 32 bytes of data:
Reply from 209.165.200.225: bytes=32 time=5ms TTL=254
Reply from 209.165.200.225: bytes=32 time<1ms TTL=254
Reply from 209.165.200.225: bytes=32 time<1ms TTL=254
Reply from 209.165.200.225: bytes=32 time=10ms TTL=254

Ping statistics for 209.165.200.225:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 10ms, Average = 3ms
```

Konfiguracja DHCP, AAA, i SSH

Skonfiguruj ASA jako serwer DHCP.

Skonfiguruj pulę adresów DHCP i uaktywnij ją na wewnętrznym interfejsie ASA. Jest to zakres adresów, które mają być przypisane do klientów DHCP. Spróbuj ustawić zakres od 192.168.1.5 do 192.168.1.100:

```
ASA-CS(config)# 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
```

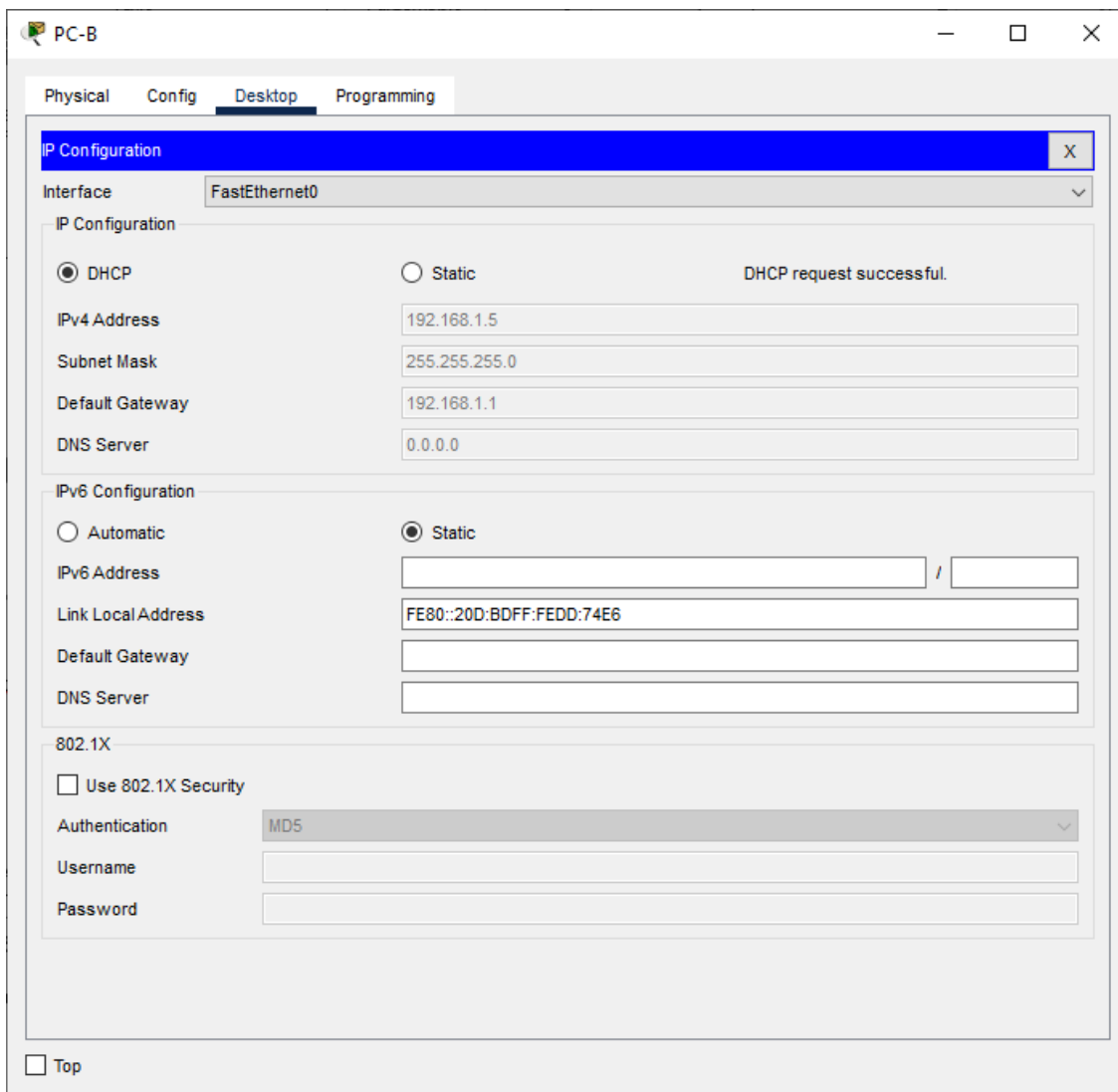
Powtórz polecenie **dhcpd** i określ pulę jako 192.168.1.5-192.168.1.36

```
ASA-CS(config)# dhcpd address 192.168.1.5-192.168.1.36 inside
```


Włącz usługę DHCP w ramach ASA, aby urządzenie mogło nasłuchiwać żądań klientów DHCP na interfejsie wewnętrznym:

```
ASA-CS (config) # dhcpd enable inside
```

Zmień konfigurację komputera PC-B tak, aby automatycznie uzyskiwał on adres IP z serwera DHCP ASA:



The screenshot shows the 'PC-B' configuration window with the 'Desktop' tab selected. The 'IP Configuration' section for 'FastEthernet0' is active. Under 'IP Configuration', the 'DHCP' radio button is selected, and a message 'DHCP request successful.' is displayed. The 'IPv4 Address' is set to '192.168.1.5', 'Subnet Mask' to '255.255.255.0', 'Default Gateway' to '192.168.1.1', and 'DNS Server' to '0.0.0.0'. The 'IPv6 Configuration' section shows 'Static' selected. The '802.1X' section has 'Use 802.1X Security' unchecked, 'Authentication' set to 'MD5', and empty fields for 'Username' and 'Password'. A 'Top' link is at the bottom left.

Konfiguracja lokalnej bazy AAA do uwierzytelniania użytkowników

Zdefiniuj użytkownika lokalnego o nazwie **admin**, korzystając z polecenia **username**. Podaj hasło **ciscoASA**:

```
ASA-CS (config) # username admin password ciscoASA
```

Skonfiguruj AAA do korzystania z lokalnej bazy danych ASA do uwierzytelniania użytkowników SSH

```
ASA-CS (config) # aaa authentication ssh console LOCAL
```

Konfiguracja zdalnego dostępu SSH do ASA.

Wygeneruj parę kluczy RSA, która jest wymagana do obsługi połączeń SSH:

```
ASA-CS (config) # crypto key generate rsa modulus 1024
```

Zapisz klucze RSA w pamięci flash za pomocą polecenia **copy run start** lub **write mem**:

```
ASA-CS (config) # write mem
```

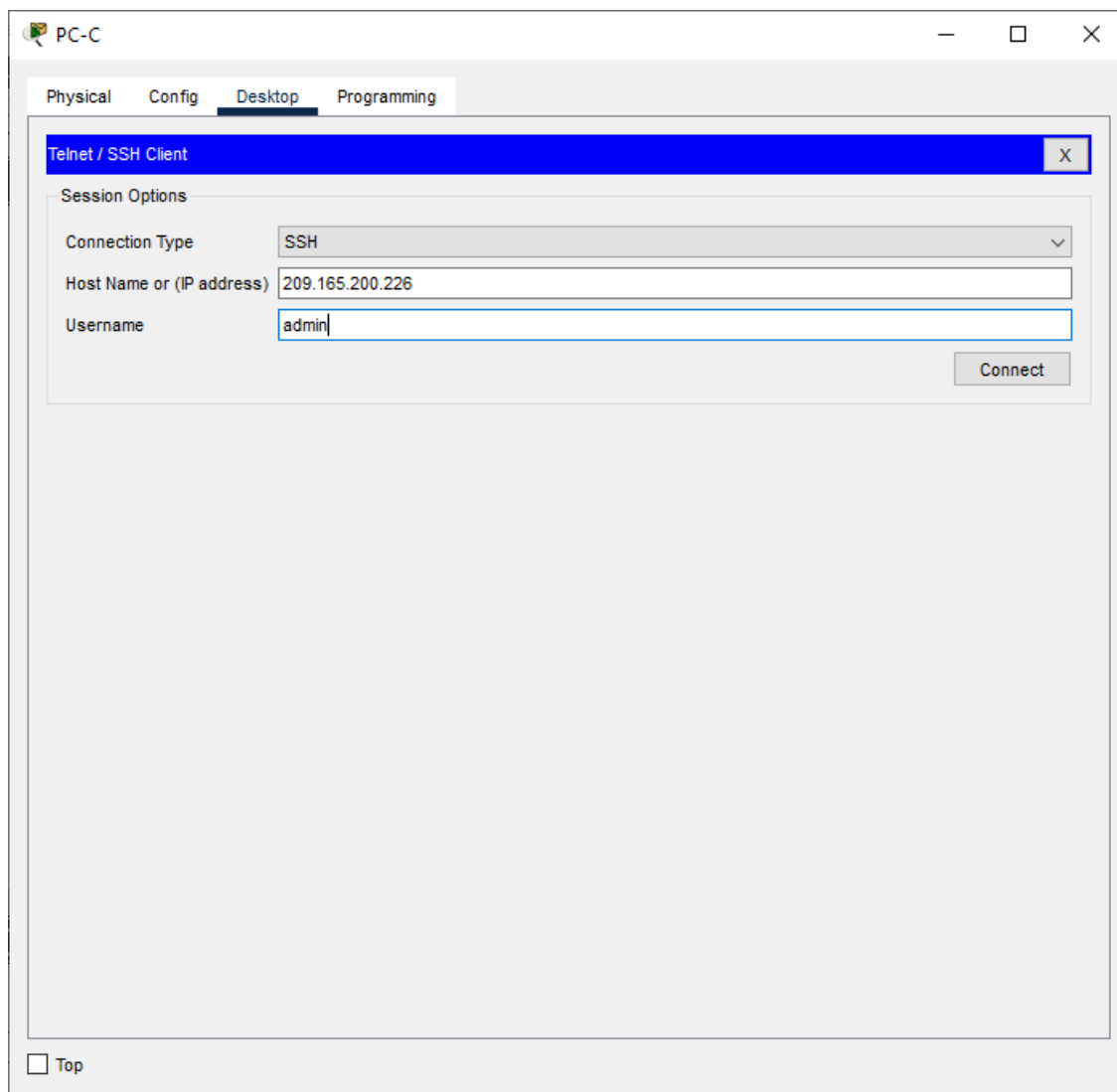
Skonfiguruj ASA tak, aby możliwe było zestawianie połączenia SSH z dowolnego hosta w sieci wewnętrznej (192.168.1.0/24) oraz z hosta zarządzania w sieci zewnętrznej (172.16.3.3). Ustaw limit czasu SSH na 10 minut (wartość domyślna to 5 minut).

```
ASA-CS (config) # ssh 192.168.1.0 255.255.255.0 inside
```

```
ASA-CS (config) # ssh 172.16.3.3 255.255.255.255 outside
```

```
ASA-CS (config) # ssh timeout 10
```

Na PC-C użyj klienta SSH, aby połączyć się z zewnętrznym interfejsem ASA pod adresem IP 209.165.200.226. Przy pierwszym połączeniu klient SSH może zostać poproszony o zaakceptowanie klucza hosta RSA serwera ASA SSH. Zaloguj się jako użytkownik **admin** i podaj hasło **ciscoASA**. Możesz również połączyć się z wewnętrznym interfejsem ASA, korzystając z klienta SSH na komputerze PC-B, używając adresu IP 192.168.1.1.



Konfigurowanie DMZ, statycznego NAT i list kontroli dostępu (ACL)

Konfiguracja strefy zdemilitaryzowanej DMZ na interfejsie VLAN 3 urządzenia ASA.

Skonfiguruj interfejs DMZ VLAN 3, czyli miejsce, w którym będzie znajdować się publiczny serwer sieciowy. Przypisz adres IP 192.168.2.1/24 do interfejsu VLAN 3, nazwij go **dmz** i przypisz poziom bezpieczeństwa **70**.

```
ASA-CS (config) # interface vlan 3  
ASA-CS (config-if) # ip address 192.168.2.1 255.255.255.0  
ASA-CS (config-if) # nameif dmz
```



```
ERROR: This license does not allow configuring more than 2
interfaces with
nameif and without a "no forward" command on this interface or on
1 interface(s) with nameif already configured.
ASA-CS(config-if)# no forward interface vlan 1
ASA-CS(config-if)# nameif dmz
INFO: Security level for "dmz" set to 0 by default.
ASA-CS(config-if)# security-level 70
ASA-CS(config-if)# no shut
```

Przypisz fizyczny interfejs ASA E0/2 do DMZ VLAN 3 i włącz interfejs:

```
ASA-CS(config)# interface Ethernet0/2
ASA-CS(config-if)# switchport access vlan 3
ASA-CS(config-if)# no shut
```

Wyświetl stan wszystkich interfejsów ASA za pomocą polecenia **show interface ip brief**:

```
ASA-CS# show interface ip brief
```

Interface Protocol	IP-Address	OK?	Method	Status
Ethernet0/0 up	unassigned	YES	unset	up
Ethernet0/1 up	unassigned	YES	unset	up
Ethernet0/2 up	unassigned	YES	unset	up
Ethernet0/3 down	unassigned	YES	unset	down
Ethernet0/4 down	unassigned	YES	unset	down
Ethernet0/5 down	unassigned	YES	unset	down

Ethernet0/6 down	unassigned	YES unset	down
Ethernet0/7 down	unassigned	YES unset	down
Vlan1 up	192.168.1.1	YES CONFIG	up
Vlan2 up	209.165.200.226	YES manual	up
Vlan3 up	192.168.2.1	YES manual	up

Wyświetl informacje dotyczące interfejsów VLAN za pomocą polecenia **show ip address**:

ASA-CS# **show ip address**

System IP Addresses:

Interface Method	Name	IP address	Subnet mask
Vlan1 255.255.255.0	inside CONFIG	192.168.1.1	
Vlan2 255.255.255.248	outside manual	209.165.200.226	
Vlan3 255.255.255.0	dmz manual	192.168.2.1	

Current IP Addresses:

Interface Method	Name	IP address	Subnet mask
Vlan1 255.255.255.0	inside CONFIG	192.168.1.1	
Vlan2 255.255.255.248	outside manual	209.165.200.226	
Vlan3 255.255.255.0	dmz manual	192.168.2.1	

Wyświetl sieci VLAN i przypisania portów w ASA za pomocą polecenia **show switch vlan**:

```
ASA-CS# show switch vlan
```

VLAN	Name	Status	Ports
1	inside	up	Et0/1, Et0/3, Et0/4, Et0/5
2	outside	up	Et0/6, Et0/7 Et0/0
3	dmz	up	Et0/2

Konfiguracja statycznej translacji adresów NAT z wykorzystaniem obiektów sieciowych.

Skonfiguruj obiekt sieciowy o nazwie **dmz-server** i przypisz mu statyczny adres IP serwera DMZ (192.168.2.3). W trybie konfiguracji obiektu sieciowego, użyj polecenia **nat**, aby określić, że ten obiekt jest używany do translacji adresu DMZ na adres zewnętrzny za pomocą statycznego NAT. Jako adres publiczny ustaw 209.165.200.227.

```
ASA-CS (config)# object network dmz-server
```

```
ASA-CS (config-network-object)# host 192.168.2.3
```

```
ASA-CS (config-network-object)# nat (dmz,outside) static  
209.165.200.227
```

Konfiguracja listy kontroli dostępu w celu umożliwienia dostępu do serwera w DMZ z sieci publicznej

Skonfiguruj nazwaną listę dostępu (OUTSIDE-DMZ), która zezwala na korzystanie z dowolnych protokołów stosu TCP/IP w komunikacji urządzeń sieci zewnętrznej (publicznej) z serwerem w sieci DMZ. Nałóż listę kontroli dostępu na zewnętrznym interfejsie ASA w kierunku IN.

```
ASA-CS (config)# access-list OUTSIDE-DMZ permit ip any host  
192.168.2.3
```

```
ASA-CS (config)# access-group OUTSIDE-DMZ in interface outside
```

Przetestuj dostęp do serwera DMZ.

Utwórz interfejs pętli zwrotnej o numerze 0 (Lo0) na routerze R2, emulujący host w sieci zewnętrznej. Przypisz adres IP 172.30.1.1 z maską 255.255.255.0 interfejsowi Lo0. Wyślij ICMP Echo Request na adres



publiczny serwera DMZ z R2 przy użyciu interfejsu pętli zwrotnej jako źródła ping. Polecenia ping powinny zakończyć się powodzeniem.

```
R2(config-if)# interface lo0
R2(config-if)# ip address 172.30.1.1 255.255.255.0
R2# ping
Protocol [ip]:
Target IP address: 209.165.200.227
Repeat count [5]:
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]: y
Source address or interface: 172.30.1.1
Type of service [0]:
Set DF bit in IP header? [no]:
Validate reply data? [no]:
Data pattern [0xABCD]:
Loose, Strict, Record, Timestamp, Verbose[none]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 209.165.200.227, timeout is 2
seconds:
Packet sent with a source address of 172.30.1.1
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/7/14
ms
```

Wykonaj polecenie ping z komputera PC-C do serwera DMZ, na jego adres publiczny 209.165.200.227. Polecenia ping powinny zakończyć się powodzeniem.



```
PC-C
Physical Config Desktop Programming
Command Prompt
Reply from 209.165.200.227: bytes=32 time=2ms TTL=124
Reply from 209.165.200.227: bytes=32 time=3ms TTL=124

Ping statistics for 209.165.200.227:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 2ms, Maximum = 11ms, Average = 5ms

C:\>ping 209.165.200.227

Pinging 209.165.200.227 with 32 bytes of data:

Reply from 209.165.200.227: bytes=32 time<1ms TTL=124
Reply from 209.165.200.227: bytes=32 time<1ms TTL=124
Reply from 209.165.200.227: bytes=32 time=13ms TTL=124
Reply from 209.165.200.227: bytes=32 time=13ms TTL=124

Ping statistics for 209.165.200.227:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 13ms, Average = 6ms

C:\>ping 209.165.200.227

Pinging 209.165.200.227 with 32 bytes of data:

Reply from 209.165.200.227: bytes=32 time<1ms TTL=124
Reply from 209.165.200.227: bytes=32 time=13ms TTL=124
Reply from 209.165.200.227: bytes=32 time=10ms TTL=124
Reply from 209.165.200.227: bytes=32 time=56ms TTL=124

Ping statistics for 209.165.200.227:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 56ms, Average = 19ms

C:\>
```

Wydaj polecenie **show xlate** na ASA, aby zobaczyć, czy wysyłane pakiety ICMP Echo Request podlegały translacji adresów

```
ASA-CS# show xlate
```

```
1 in use, 1 most used
```

```
Flags: D - DNS, e - extended, I - identity, i - dynamic, r -  
portmap, s - static, T - twice, N - net-to-net
```

```
NAT from dmz:192.168.2.3/32 to outside:209.165.200.227/32 flags s  
idle 00:16:52, timeout 0:00:00
```