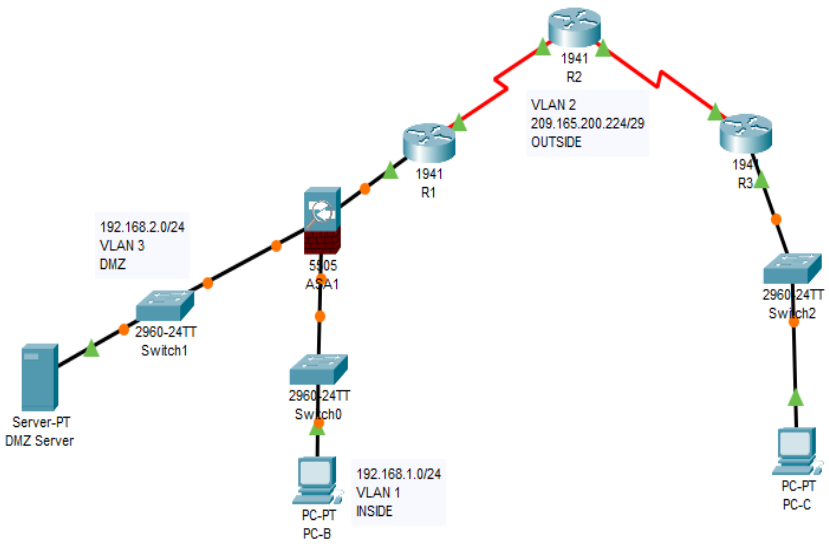
Bezpieczeństwo sieci komputerowych
Temat: Konfiguracja sprzętowego firewalla

Data: 02/06/2022
Ewa Namysł
Informatyka stosowana, III rok

1. Opis i cel zadania:

Zadanie polega na ustawieniu w Packet Tracerze topologii przedstawionej na rysunku oraz konfiguracji firewalla. Należy sprawdzić połączenia, skonfigurować ASA (Adaptive Security Appliances), routing, NAT, DHCP, AAA (Authentication, Authorization, Accounting), DMZ, static NAR i ACL (Access Control List).



2. Połączenie i konfiguracja ASA:

Adaptive Security Appliances to urządzenia sieciowe, których zadaniem jest ochrona sieci i blokowaniu niedozwolonego ruchu sieciowego, pełnią rolę firewalla.

Aby sprawdzić połączenie używamy komendy *ping*. Informacje związane np. z wersjami sprawdzamy tak jak w innych urządzeniach Cisco (*show version).*

W ASA tworzymy dwa logiczne interfejsy – inside oraz outside. Dla outside ustalamy najniższy poziom bezpieczeństwa (0), dla inside najwyższy (100).
Najwyższy poziom bezpieczeństwa jest zwykle używany dla LANów i domyślnie pozwala naszej sieci na przesyłanie informacji do innych interfejsów. Z kolei najniższy poziom 0 jest przypisywany sieciom zewnętrznym i nie pozwala na przesyłanie informacji do naszej sieci wewnętrznej, jeśli nie zezwolimy na to w access-list.

3. Konfiguracja routingu oraz NAT:

Aby umożliwić ASA dostęp do zewnętrznych sieci należy skonfigurować routing statyczny, przypisać go do interfejsu outside oraz stworzyć network object i przypisać atrybuty używając *subnet* i *nat*. Umożliwi to translacja adresów sieciowych - NAT polega na zamianie adresów prywatnych lub wewnętrznych na publiczne lub globalnie routowalne adresy IP.

4. Modular Policy Framework:

Konfiguracja MPF pozwala na zdefiniowanie zasad dla firewalla. Trzy główne komponenty MPF to: Class Map, Policy Map i Service Map.

- Class Map służy do identyfikacji rodzaju ruchu sieciowego.
- Policy Map ustala jakie działania podejmuje ASA względem ruchu zdefiniowanego w Class Map.
- Service Policy określa gdzie obowiązują ww. zasady (np. konkretny interfejs etc.)

5. DHCP, AAA, SSH:

Wykorzystujemy ASA jako serwer DHCP i ustawiamy zakres adresów dla interfejsu inside:

dhcpd address 192.168.1.5-192.168.1.36 inside
dhcpd enable inside

AAA (Authentication, Authorization, Accounting) jest metodą weryfikacji userów i może być oparta na lokalnej bazie użytkownikach.

- Authentication – sprawdzenie wiarygodności użytkownika
- Authorization – weryfikacja zasobów do których dostęp ma dany użytkownik
- Accounting – zbieranie i zapisywanie informacji o akcjach podjętych przez użytkownika

Aby skonfigurować AAA na ASA, żeby wykorzystywała lokalną bazę danych dla połączeń przez SSH wpisujemy:

aaa authentication ssh console LOCAL

Następnie konfigurujemy dostęp do ASA poprzez SSH. Generujemy klucz RSA i ustalamy dostęp do SSH dla wszystkich z sieci inside i wybranych komputerów z sieci outside:

ssh 192.168.1.0 255.255.255.0 inside
ssh 172.16.3.3255.255.255.255 outside

6. DMZ, static NAT, ACL:

DMZ (strefa zdemilitaryzowana) to wydzielony w firewallu obszar sieci, który nie należy ani do sieci wewnętrznej, ani zewnętrznej. Są tam umieszczane serwery, których usługi mają kontakt z siecią zewnętrzną (np. serwery FTP, web, poczty elektronicznej etc.), ale ze względu na bezpieczeństwo są odseparowane od sieci wewnętrznej. W przypadku włamania na serwer w DMZ, nie ma możliwości przedostania się do sieci wewnętrznej.

Tworzymy interfejs VLAN dla DMZ i zamykamy przekierowywanie do interfejsu inside:

no forward interface vlan 1

Security level ustawiamy na 70. Oznacza to, że możliwy jest ruch sieciowy z sieci wewnętrznej do DMZ oraz z DMZ do sieci zewnętrznej, ale nie z DMZ do sieci wewnętrznej bez wpisu w access-list.

Konfigurujemy statyczny NAT dla serwera w DMZ, ustalamy adres publiczny, a następnie tworzymy access-listę. W ACL zezwalamy na ruch ICMP i TCP na porcie 80 dla zewnętrznych hostów do DMZ:

access-list OUTSIDE-DMZ permit icmpany host 192.168.2.3
access-list OUTSIDE-DMZ permit tcpany host 192.168.2.3 eq 80ASA
access-group OUTSIDE-DMZ in interface outside