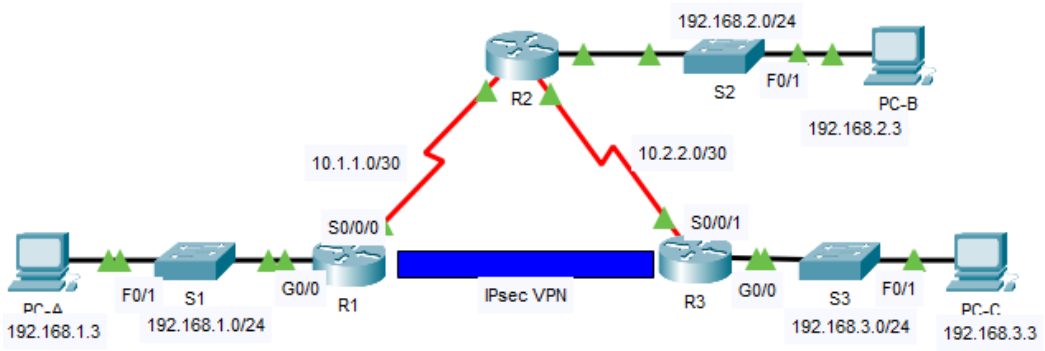
Bezpieczeństwo sieci komputerowych
Temat: VPN

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

1. Opis i cel zadania:

Zadanie polega na skonfigurowaniu VPN w przedstawionej poniżej topologii:



Tunel ma być dostępny między routerem 1 a routerem 2, a wykorzystywany jest do tego router numer 2, który nie wie o istnieniu VPNa.

2. Aktywacja modułu securityk9:

Securityk9 umożliwia m.in. enkrypcję przesyłanych danych, dzięki czemu można utworzyć bezpieczny VPN zgodnie z IPsec.
Najpierw sprawdzamy poprzez *show version* czy licencja została aktywowana na routerze. Jeśli nie, wpisujemy:

license boot module c2900 technology-package securityk9
end

Zapisujemy konfigurację i restartujemy router:

copy running-config startup-config
reload

Czynności te wykonujemy zarówno na R1, jak i na R3.

3. Access-listy:

Konfigurujemy access-listę na pozwalającą na przesyłanie z R1 do R3:

access-list 110 permit ip 192.168.1.0 0.0.0.255 192.168.3.0 0.0.0.255

Permit ip pozwala na przesyłanie informacji różnymi protokołami (tak jak permit tcp pozwala tylko na przesyłanie danych protokołem TCP).

4. Konfiguracja ISAKMP:

ISAKMP to protokół związany z autentykacją i wymianą kluczy kryptograficznych. Wpisujemy:

crypto isakmp policy 10
encryption aes
authentication pre-share
group 2
exit
crypto isakmp key cisco address 10.2.2.2

Protokół ESP zapewnia poufność, uwierzytelnianie i integralność danych – tutaj używamy esp-3des. Esp-sha-hmac to algorytm, który wykorzystywany jest w protokole ESP do uwierzytelniania danych o zmiennej długości przy pomocy klucza. Wpisujemy:

crypto ipsec transform-set VPN-SET esp-3des esp-sha-hmac
crypto map VPN-MAP 10 ipsec-isakmp
description VPN connection to R3
set peer 10.2.2.2
set transform-set VPN-SET
match address 110
exit

Na interfejsie wychodzącym S0/0/0:

crypto map VPN-MAP

5. Konfiguracja drugiego routera:

Aby VPN działał poprawnie, należy skonfigurować drugi router w ten sam sposób, podmieniając adresy. Na routerze R3 uzupełniamy access-listę:

access-list 110 permit ip 192.168.3.0 0.0.0.255 192.168.1.0 0.0.0.255

Przy konfiguracji ISAKMP podmieniamy adres 10.1.1.2 na 10.0.0.2.

6. Enkrypcja pakietów:

Aby sprawdzić liczbę przesłanych pakietów, które zostały zaszyfrowane wpisujemy na jednym z routerów:

show crypto ipsec sa

Po poprawnym skonfigurowaniu VPN informacje przesyłane z komputera C do komputera A są szyfrowane. Z kolei pakiety z komputera B do C nie, ponieważ komputery te nie należą do wspólnej wirtualnej sieci prywatnej.