Ćwiczenie 12 Konfigurowanie i testowanie VPN (PPTP)

W czasie realizacji ćwiczenia należy opracowywać sprawozdanie według załączonego wzoru, zawierające obrazy odpowiednich okien, oraz wnioski i komentarze dotyczące realizowanych zadań.
Sprawozdanie w postaci elektronicznej należy oddać prowadzącemu zajęcia przed opuszczeniem laboratorium.

Zadanie 1 Konfigurowanie serwera VPN-PPTP.

Ćwiczenie to powinno zostać zrealizowane na jednym z komputerów partnerskich.

1. Jeżeli protokół TCP/IP jest konfigurowany dynamicznie, to zmienić konfigurację na statyczną , nadając komputerowi adres *192.168.x.nr_serwera*. Wartość x poda prowadzący. Maskę podsieci ustawić na wartość 255.255.0.0. Jeżeli będą potrzebne inne parametry, to poda je prowadzący zajęcia.
2. W grupie narzędzi administracyjnych otworzyć konsolę ***Routing i dostęp zdalny*** (*Routing and Remote Access*). W menu podręcznym ikony z nazwą serwera, wybrać polecenie ***Konfiguruj i włącz routing i dostęp zdalny*** (*Configure and Enable Routing and Remote Access)*, powodujące uruchomienie odpowiedniego kreatora.
3. Na stronie ***Konfiguracja*** wybrać opcję ***Konfiguracja niestandardowa***.
4. Na stronie ***Konfiguracja niestandardowa*** zakreślić opcję ***Dostęp przez sieć VPN***.
5. Kończąc pracę kreatora, uruchomić usługę RRAS.
6. W konsoli ***Routing i dostęp zdalny*** (*Routing and Remote Access*), w menu podręcznym ikony serwera wybrać funkcję ***Właściwości***.
7. W oknie zakładki ***Ogólne***, powinno być zakreślone pole ***Serwer zdalnego dostępu***, a pole ***Router*** – wyczyszczone. Po zaakceptowaniu zmian zezwolić na restart usługi RRAS.
8. W oknie zakładki ***Protokół IP***, określić statyczną pulę adresów przydzielanych klientom. Pula powinna zawierać 10 adresów począwszy od 10.100.100.100.

9. W konsoli ***Zarządzanie komputerem***, w oknie właściwości konta administratora, pod zakładką ***Telefonowanie*** zakreslić opcję ***Zezwalaj na dostęp***.
10. Otworzyć i zostawić otwarty kontener ***Porty*** w przystawce ***Routing i dostęp zdalny***.
11. Odświeżyć obraz w konsoli RRAS.
12. Przy pomocy polecenia ***ipconfig /all*** (z linii poleceń) wyświetlić informację o konfiguracji interfejsu sieciowego.
13. Przy pomocy polecenia ***route*** (z linii poleceń) wyświetlić zawartość tablicy routingu.

Zadanie 2 Konfigurowanie klienta VPN-PPTP.

Ćwiczenie to powinno zostać zrealizowane na drugim z komputerów partnerskich.

1. Jeżeli protokół TCP/IP jest konfigurowany dynamicznie, to zmienić konfigurację, nadając komputerowi adres *192.168.x.nr_klienta*. Maskę podsieci ustawić na wartość 255.255.0.0. Jeżeli będą potrzebne inne parametry, to poda je prowadzący zajęcia.
2. Przy pomocy polecenia ***ipconfig /all*** (z linii poleceń) wyświetlić informację o konfiguracji

interfejsu sieciowego.
3. Przy pomocy polecenia ***route*** (z linii poleceń) wyświetlić zawartość tablicy routingu.

4. W panelu sterowania otworzyć okno ***Połączenia sieciowe*** i uruchomić kreator nowego połączenia.
5. Na stronie ***Typ połączenia sieciowego*** wybrać opcję ***Połącz z siecią w miejscu pracy***.
6. Na stronie ***Połączenie sieciowe*** wybrać opcję ***Połączenie wirtualnej sieci prywatnej***.
7. Na stronie ***Nazwa połączenia*** wpisać VPN_DO_*nazwa serwera partnera*.
8. Na stronie ***Wybór serwera sieci VPN*** wpisać adres komputera partnera, który pełni rolę serwera VPN.
9. Na stronie ***Dostępność połączeń*** wybrać opcję ***Do użytku wszystkich***.
10. Po zakończeniu pracy kreatora zamknąć okno umożliwiające podłączenie się do serwera.

Zadanie 3 Testowanie połaczenia VPN-PPTP.

1. Jeżeli nie są jeszcze zainstalowane, to zainstalować pakiet ***WinPcap*** i *sniffer* ***Ethereal***.
2. Na obu komputerach uruchomić *sniffer*. W razie potrzeby zdefiniować odpowiednie filtry.
3. Na komputerze klienta VPN, w oknie ***Połaczenia sieciowe***, w menu podręcznym połączenia VPN_DO_*nazwa serwera partnera* wybrać funkcję ***Połącz***. Wpisać nazwę konta i hasło administratora. Na obu komputerach zaobserwować proces połączenia w oknie sniffera.
4. Po nawiązaniu połączenia, na obu komputerach, w oknach wiersza poleceń wydać polecenie ***ipconfig*** a następnie ***route***.
5. Odświeżyć zawartość okna konsoli ***Routing i dostęp zdalny*** (*Routing and Remote Access*) na serwerze VPN. Zapoznać się również z zawartością kontenera ***Klienci zdalnego dostępu***.
6. Obserwując zawartość okna sniffera, sprawdzić poprawność komunikacji (w obie strony) pomiędzy komputerami partnerskimi przy pomocy programu ***ping*** wykorzystując oba dostępne na każdym komputerze interfejsy sieciowe. UWAGA: przed każdym badaniem połączenia (uruchomieniem polecenia *ping*), na nowo uruchamiać sniffer.
7. Na komputerze klienta VPN, w oknie ***Połaczenia sieciowe***, w menu podręcznym połączenia VPN_DO_*nazwa serwera partnera* wybrać funkcję ***Rozłącz***. Na obu komputerach, w oknie sniffera zaobserwować przebieg rozłączania.
8. Odświeżyć zawartość okna konsoli ***Routing i dostęp zdalny*** (*Routing and Remote Access*) na serwerze VPN.
9. Na komputerze klienta VPN, w oknie ***Połaczenia sieciowe*** skasować definicję połączenia VPN.
10. Na komputerze serwera VPN, w oknie konsoli ***Routing i dostęp zdalny*** (*Routing and Remote Access*), w menu podręcznym pozycji odpowiadającej serwerowi VPN wybrać opcję ***Wyłącz routing i dostęp zdalny*** (*Disable Routing and Remote Access)*.
11. Przy pomocy polecenia ***ipconfig*** (z linii poleceń) wyświetlić informację o konfiguracji interfejsu sieciowego na obu komputerach.
12. Przy pomocy polecenia ***route*** (z linii poleceń) wyświetlić zawartość tablic routingu na obu komputerach.