Ćwiczenie 07b Konfigurowanie i testowanie VPN (PPTP)

Celem ćwiczenia jest zapoznanie studentów z przykładową procedurą tworzenia i testowania kanału VPN (protokół PPTP) w systemie Windows. Realizowane zadania obejmują skonfigurowanie kanału VPN pomiędzy dwoma komputerami partnerskimi a następnie testowanie poprawności pracy utworzonego kanału. W czasie testowania studenci „podglądają" przy pomocy snifera ruch sieciowy w takim kanale i porównują go z ruchem sieciowym pomiędzy komputerami w przypadku, gdy kanał VPN nie został skonfigurowany lub zabezpieczenia zostały wyłączone.

W ramach przygotowania do ćwiczenia należy zapoznać się z udostępnionymi materiałami wykładowymi.

W czasie realizacji ćwiczenia należy opracowywać sprawozdanie według załączonego wzoru, zawierające obrazy odpowiednich okien, oraz wnioski i komentarze dotyczące realizowanych zadań.

Zadanie 1 Konfigurowanie serwera VPN-PPTP.

Zadanie to powinno zostać zrealizowane na jednym z wykorzystywanych systemów.

1. Według wskazówek prowadzącego, skonfigurować protokół TCP/IP. Jeżeli wskazówki nie zostaną przekazane, to do konfigurowania interfejsów sieciowych należy wykorzystać usługę DHCP.
2. Uruchomić program menedżera serwera (*Server Manager*) i dodać rolę dotyczącą zdalnego dostępu (*Remote Access*). Po zaznaczeniu tej roli, we wszystkich kolejnych oknach kreatora zaakceptować zaproponowane ustawienia.
3. Po zakończeniu instalacji, w oknie programu menedżera serwera (*Server Manager*) wybrać łącze dotyczące zdalnego dostępu (*Remote Access*).Należy teraz skonfigurować tą usługę (link na żółtym polu).
4. W oknie uruchomionego kreatora konfiguracji wybrać łącze prowadzące do konfigurowania jedynie VPN (*Deploy VPN only*).
5. Automatycznie zostanie otworzona konsola routingu i dostępu zdalnego (*Routing and Remote Access*). W menu podręcznym ikony z nazwą serwera, wybrać polecenie konfigurowania i włączenia routingu i dostępu zdalnego (*Configure and Enable Routing and Remote Access**)***. Spowoduje to uruchomienie odpowiedniego kreatora.
6. Na stronie konfiguracji *(Cofiguration)* wybrać opcję konfiguracji niestandardowej *(Custom configuration).*
7. Na kolejnej stronie zakreślić opcję dostępu przez VPN (*VPN access*).
8. Kończąc pracę kreatora, uruchomić usługę RRAS.
9. W konsoli routingu i dostępu zdalnego (*Routing and Remote Access*), w menu podręcznym ikony serwera wybrać pozycję dotyczącą właściwości (*Properties*).
10. W oknie zakładki protokołu IPv4, określić statyczną pulę adresów przydzielanych klientom. Pula powinna zawierać 10 adresów począwszy od 10.100.100.100.
11. Zamknąć okno konsoli routingu i dostępu zdalnego (*Routing and Remote Access*).
12. W grupie narzędzi administracyjnych otworzyć konsolę zarządzania komputerem (*Computer*

Management).W oknie właściwości konta administratora, pod zakładką właściwości dotyczących telefonowania (*Dial-in*) zakreślić opcję Zezwolenia na dostęp (*Allow Access*).
13. Otworzyć i zostawić otwarty kontener portów *(Ports)* w konsoli routingu i dostępu zdalnego (*Routing and Remote Access*). Odświeżyć obraz w konsoli.
14. Przy pomocy polecenia ***ipconfig /all*** (np. w oknie programu ***PowerShell***) wyświetlić informację o konfiguracji interfejsu sieciowego.
15. Przy pomocy polecenia ***route*** (np. w oknie programu ***PowerShell***) wyświetlić zawartość tablicy routingu.

Zadanie 2 Konfigurowanie klienta VPN-PPTP.

Zadanie to powinno zostać zrealizowane na drugim z wykorzystywanych systemów.

1. Według wskazówek prowadzącego, skonfigurować protokół TCP/IP. Jeżeli wskazówki nie zostaną przekazane, to do konfigurowania interfejsów sieciowych należy wykorzystać usługę DHCP.
2. Przy pomocy polecenia ***ipconfig /all*** (np. w oknie programu ***PowerShell***) wyświetlić informację o konfiguracji interfejsu sieciowego.
3. Przy pomocy polecenia ***route*** (np. w oknie programu ***PowerShell***) wyświetlić zawartość tablicy routingu.

4. W panelu sterowania otworzyć okno centrum sieci (*Network and Sharing Center*) a następnie uruchomić kreator nowego połączenia.
5. Wybrać opcję tworzenia połączenia telefonicznego lub VPN (*Connect to a workplace*).
6. Podczas pracy kreatora, w odpowiednim polu podać adres serwera zdalnego dostępu. Jako nazwę połaczenia podać: VPN_DO_*nazwa serwera.* Połączenie powinno być dostępne dla wszystkich użytkowników.

Zadanie 3 Testowanie połaczenia VPN-PPTP.

1. Na obu komputerach uruchomić *sniffer*. W razie potrzeby zdefiniować odpowiednie filtry. Ruch sieciowy należy zbierać na interfejsie fizycznym a nie wirtualnym (RAS).
2. Na komputerze klienta VPN, w oknie połączeń sieciowych (*Networks*), otworzyć zdefiniowane połączenie VPN i połączyć się z serwerem (*Connect*). Wpisać nazwę konta i hasło administratora. Na obu komputerach, w oknie sniffera, obserwować proces nawiązywania połączenia.
3. Po nawiązaniu połączenia, na obu komputerach, w oknach wiersza poleceń wydać polecenie ***ipconfig*** (np. w oknie programu ***PowerShell***) a następnie wyświetlić tablicę routingu przy pomocy polecenia ***router*** (np. w oknie programu ***PowerShell***).
4. Odświeżyć zawartość konsoli routingu i dostępu zdalnego (*Routing and Remote Access*) na serwerze VPN. Zapoznać się również z zawartością kontenera klientów zdalnego dostępu (*Remote Access Clients*).
5. Obserwując zawartość okna sniffera, sprawdzić poprawność komunikacji (w obie strony) pomiędzy komputerami partnerskimi przy pomocy programu ***ping*** (np. w oknie programu

PowerShell) wykorzystując oba dostępne na każdym komputerze interfejsy sieciowe. UWAGA: przed każdym badaniem połączenia (uruchomieniem polecenia *ping*), na nowo uruchamiać sniffer.

6. Na komputerze klienta VPN, w oknie połączeń sieciowych (*Networks*) dokonać rozłączenia połączenia VPN. Na obu komputerach, w oknie sniffera zaobserwować przebieg rozłączania.
7. Odświeżyć zawartość konsoli routingu i dostępu zdalnego (*Routing and Remote Access*) na serwerze VPN.
8. Na komputerze klienta VPN, w panelu sterowania otworzyć centrum sieci (*Network and Sharing Center*).
9. Wybrać łącze umożliwiające zmianę ustawień adaptera (*Change adapter settings*).
10. W menu podręcznym ikony zdefiniowanego połączenia VPN wybrać funkcję kasowania i skasować definicję połączenia VPN.
11. Na komputerze serwera VPN, w oknie konsoli routingu i dostępu zdalnego (*Routing and Remote Access*), w menu podręcznym pozycji odpowiadającej serwerowi VPN wybrać opcję wyłączenia routingu i dostępu zdalnego (*Disable Routing and Remote Access)*.
7. Przy pomocy polecenia ***ipconfig*** (np. w oknie programu ***PowerShell***) wyświetlić informację o konfiguracji interfejsu sieciowego na obu komputerach.
8. Przy pomocy polecenia ***route*** (np. w oknie programu ***PowerShell***) wyświetlić zawartość tablic routingu na obu komputerach.