Zdalny dostęp

Zagadnienia

- VPN
- Zdalny pulpit
- VNC
- Tunelowanie przez SSH

Do przygotowania:

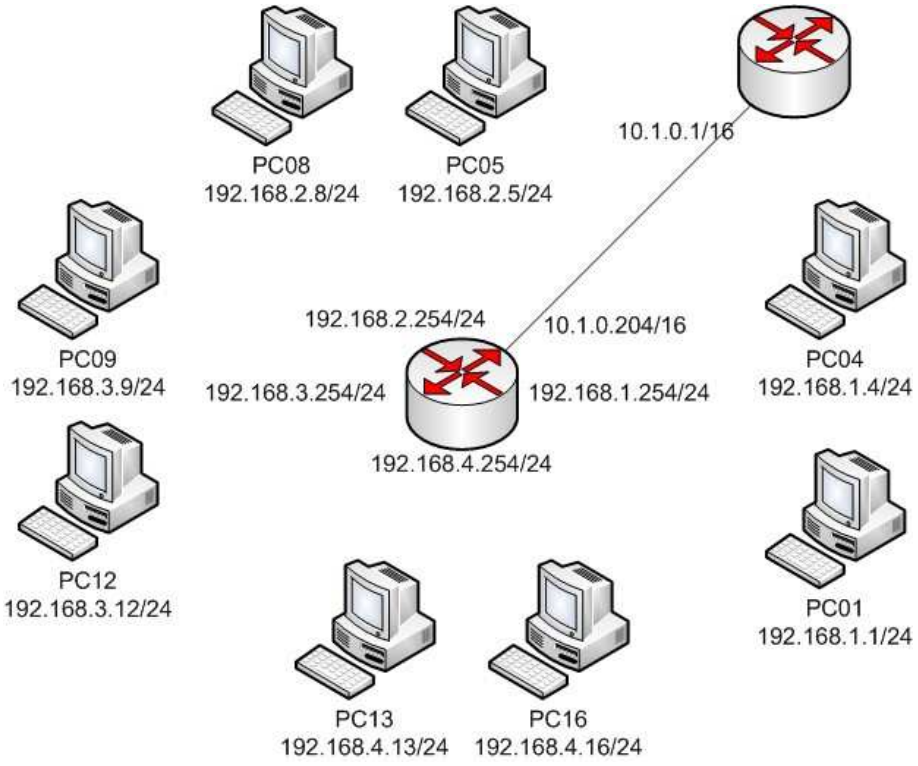
zapoznać się z dokumentacją usług VNC, Remote Desktop, VNC i przykładami konfiguracji pakietu OpenVPN (http://openvpn.net).

Punktacja:

wykonanie zadań, test na zakończenie zajęć.

Przykładowe pytania:

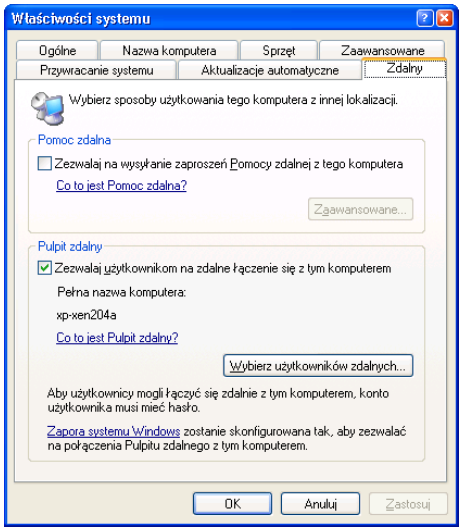
- ile równoczesnych sesji zdalnego pulpitu można nawiązać ze stacją roboczą MS Windows
- podaj port/protokół standardowej konfiguracji usługi (jedna z OpenVPN, RDP, VNC, SSH)
- wskaż usługi zdalnego dostępu zabezpieczające połączenia kryptograficznie.

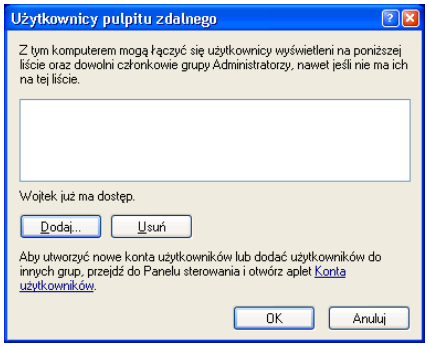


Zadania - Zdalny dostęp do stacji roboczych

1. Zdalny pulpit (ang. *Remote Desktop*)

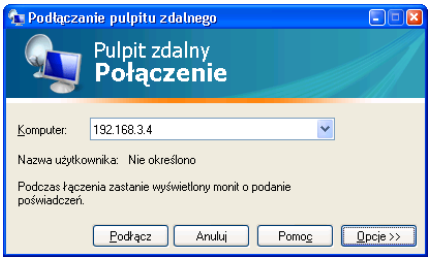
a. Uruchomić usługę zdalnego pulpitu

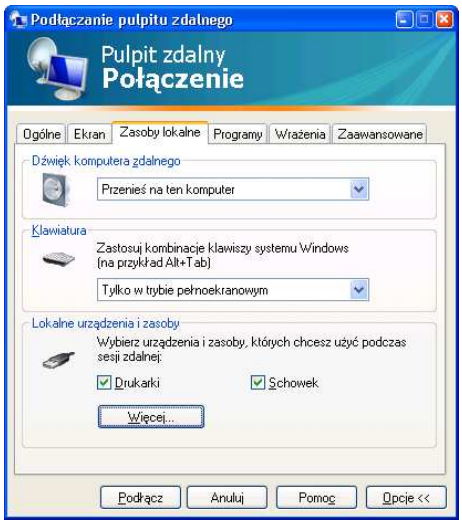


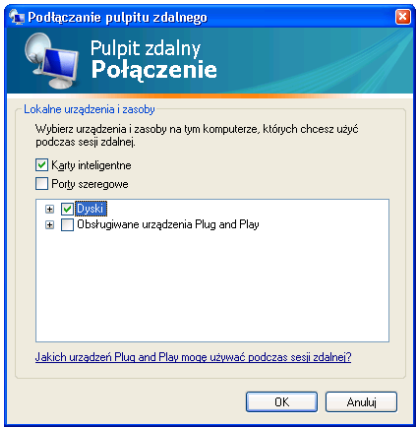


b. Utworzyć użytkownika z hasłem i przypisać go do grupy Uzytkownicy pulpitu zdalnego

c. Wykonać test połączenia







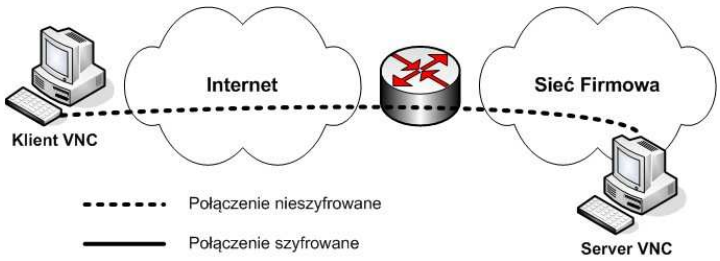
d. Zmierzyć średnie zapotrzebowanie na przepustowość łącza np. w czasie 1 min edycji tekstu w programie WordPad

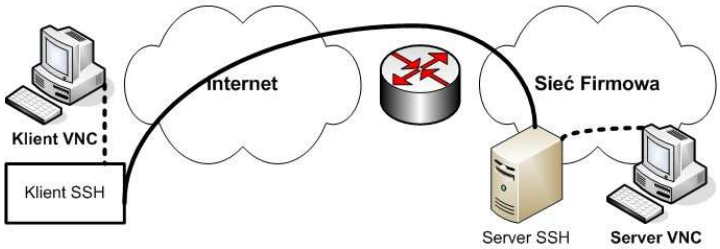
e. Wykonać test kilku równoczesnych połączeń

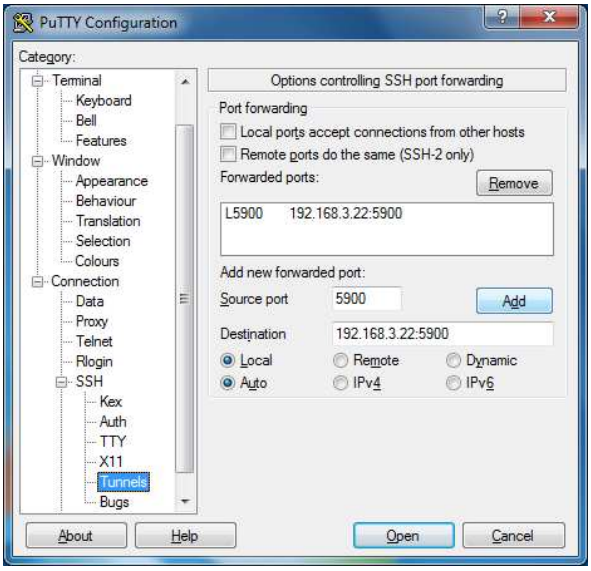
2. VNC (ang. *Virtual Network Computing*)

a. Zainstalować TightVNC
b. Uruchonić i skonfigurować Server VNC
   i. Przypisać hasło pełnego dostępu i hasło podglądu
c. Wykonać test połączenia klienta VNC
d. Wykonać test połączenia klienta za pomocą wbudowanego serwera HTTP (http://AdresIP:5800)
e. Zmierzyć średnie zapotrzebowanie na przepustowość łącza w czasie 1 min edycji tekstu w programie WordPad
f. Wykonać test kilku równoczesnych połączeń do jednego serwera VNC

3. Tunelowanie usługi (na przykładzie tunelu dla VNC po SSH)







a. Skonfigurować tunel SSH w programie PUTTY pomiędzy lokalnym portem 5900 a portem 5900 klienta VNC
b. Przetestować połączenie (adres klienta to teraz localhost)
   Uwaga: w czasie połączenia VNC nie można zamykać sesji SSH programu PUTTY. Na kliencie należy wyłączyć serwer VPN - nie ma możliwości dwukrotnego otwarcia portu 5900.

Zdalny dostęp do sieci firmowej

4. VPN (ang. *Vitrual Private Network*)

Tworzymy połączenia VPN pomiędzy oddalonymi klientami, a siecią firmową z przekierowaniem domyślnej bramy klienta na bramę firmową.

a. Zainstalować OpenVPN
b. Wygenerować zestaw certyfikatów zabezpieczających połączenie (tylko na serwerze VPN)
    i. W folderze ”C:\Program Files\OpenVPN\easy-rsa\” uruchomićw wierszu poleceń kolejno:
        1. Init-config
        2. Vars
        3. Clean-all
        4. Build-ca
        5. Build-dh
        6. Build-key-server <nazwa-certyfikatu-serwera>
        7. Build-key <nazwa-certyfikatu-klienta>
    ii. Generację certyfikatów klienta powtórzyć dla wszystkich klientów
    iii. Podczas generacji certyfikatów pamiętać należy o podawaniu identycznych danych Country, State, Organization i OrganizationUnit, a Common Name - różne.
    iv. Skopiować wygenerowane certyfikaty serwera (ca.crt, dh1024.pem, server.crt i server.key) do folderu ..\config\
    (Kopiowanie można wykonąć używając zasobów administracyjnych np. \\192.168.3.3\c$)
    v. Skopiować wygenerowane certyfikaty klientów wraz z certyfikatem centrum autoryzacyjnego (ca.crt, klient01.crt, klient01.key) do folderów ..\config\ na stacjach klienckich
c. Skopiować domyślną konfigurację z folderu ..\sample-config\ do folderu ..\config
    Uwaga: Tylko odpowiednią konfigurację - serwera albo klienta
    i. Poprawić w konfiguracjach serwera i klientów nazwy certyfikatów i kluczy - opcje **cert** i **key**
    ii. W konfiguracji serwera wymusić zmianę bramy domyślnej po podłączeniu klienta – uaktywnić opcję: **push "redirect-gateway def1 bypass-dhcp"**
    iii. Opcjonalnie ustawić klientowi serwer DNS
    uaktywnić opcję: **push "dhcp-option DNS 153.19.250.100"**
    iv. W konfiguracji klienta prawidłowo podać adres servera VPN – opcja **remote**
d. Zezwolić na serwerze na korzystanie z połączenia internetowego interfejsu eth0
e. Uruchomić OpenVPNGUI, a następnie nawiązać połączenia dla serwera i klientów
f. Sprawdzić łączność, skontrolować trasę pakietów do wybranej witryny internetowej
g. Sprawdzić bezpieczeństwo transmisji poprzez inspekcję zawartości pakietów transmitowanych od/do klienta w czasie np. oglądania witryn internetowych (Wireshark)

5. Zakończenie ćwiczenia

Po zakończeniu ćwiczenia

a. usuwamy konto użytkownika zdalnego pulpitu
b. odinstalowujemy TightVNC
c. odinstalowujemy OpenVPN
d. usuwamy folder ”C:\ProgramFiles\OpenVPN\”
e. przywracamy automatyczną konfigurację interfejsu eth0 przez DHCP