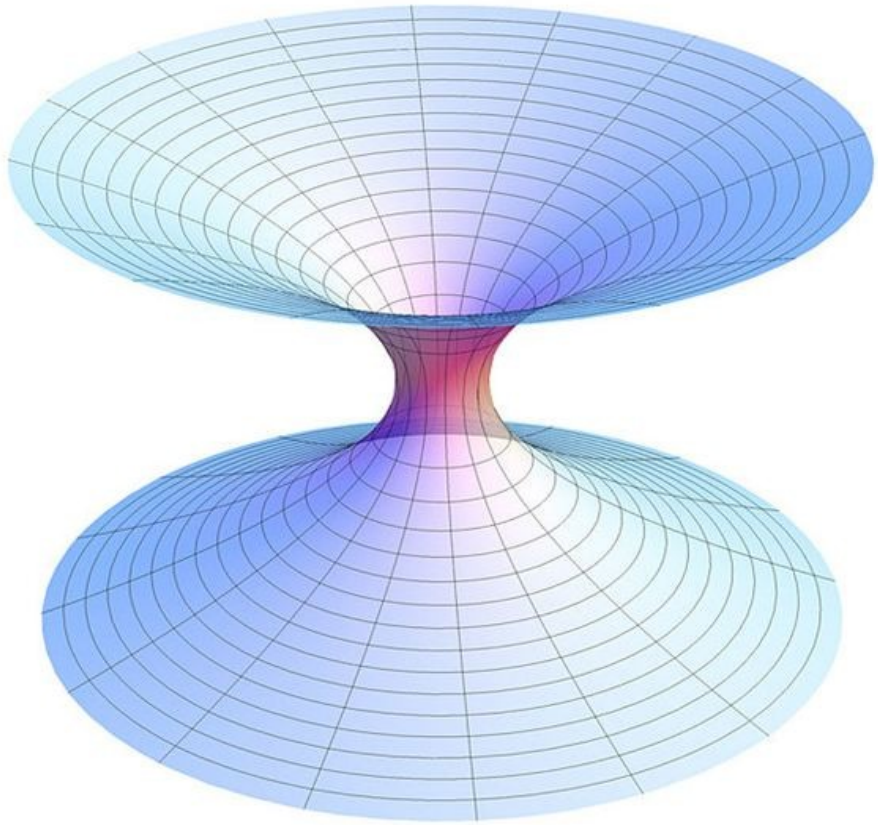
Old Man GURU Magazine

Wychodzi bardzo nieregularnie, kiedy wydaje mi się, że mam coś ciekawego lub pożytecznego do napisania...

Wydanie specjalne 10/2011 4 Maj 2011

Virtual Desktop Infrastructure

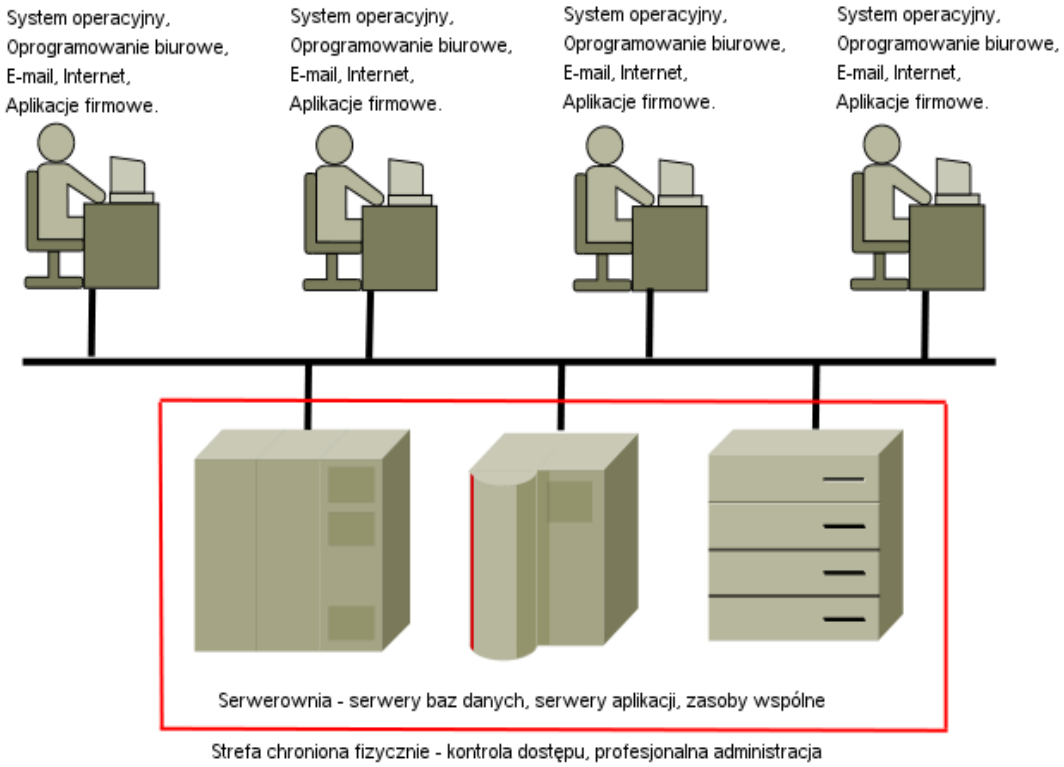
Bezpieczny tunel do świata swobodnego wyboru



Celem budowy systemu ICT jest usprawnienie procesów biznesowych realizowanych przez organizację. Duże znaczenie ma również optymalizacja kosztów oraz efektywne wykorzystywanie zasobów. Prowadzi to do konsolidacji systemów IT, czego znakomitym przykładem jest rosnąca popularność rozwiązań zwirtualizowanych oraz komputerów kasetowych (blade).

Korzyści z wprowadzania takich rozwiązań są już dość dobrze rozpoznane.

W wielu profesjonalnych systemach IT w dalszym ciągu wykorzystuje się klasyczną architekturę klient-serwer, której najistotniejszą cechą jest rozproszone przetwarzanie informacji:



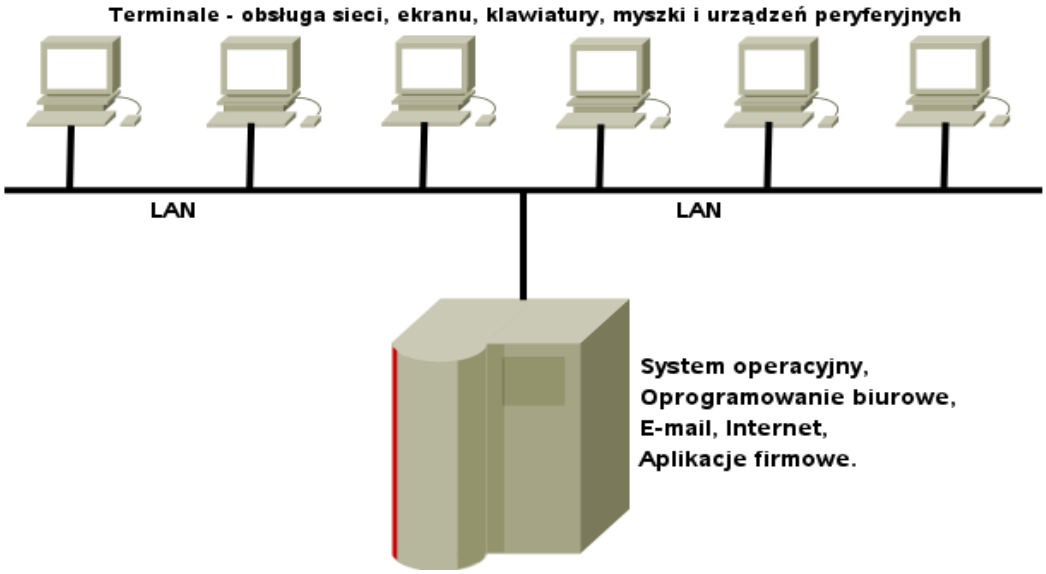
Rysunek 1
Uproszczony schemat typowej architektury klient-serwer

Podstawową cechą architektury klient-serwer jest transmisja plików pomiędzy serwerami i komputerami PC. Pobrane pliki są przetwarzane przez oprogramowanie pracujące na komputerze osobistym użytkownika. Transmisje plikowe stawiają określone wymagania sieci komputerowej, co prowadzi do wzrostu jej prędkości. O ile sieć lokalna organizacji może spełnić te wymagania ze znacznym zapasem, o tyle w sieciach rozległych zachowanie tak dużych prędkości choć technicznie możliwe jest jednak bardzo kosztowne.

Istnieje sporo rozwiązań, których dostawcy deklarują zwiększenie przepustowości transmisji plikowych w sieciach WAN, jednak ich instalacja również wiąże się ze znacznymi kosztami, a co gorsza skutek bywa niepewny.

Niejako przeciwieństwem architektury klient-serwer są rozwiązania terminalowe. Były one stosowane w systemach obsługiwanych przez duże maszyny (MainFrame) oraz systemy klasy UNIX (MidRange). Jednakże w większości przypadków stosowano terminale znakowe, system X Window oraz korzystające z niego środowiska graficzne znalazły dość ograniczone zastosowanie (głównie na uczelniach i w ośrodkach badawczych). Upowszechnienie się komputerów osobistych oraz rozwój środowiska graficznego i systemu MS Windows spowodowały znaczne ograniczenie wykorzystywania systemów terminalowych.

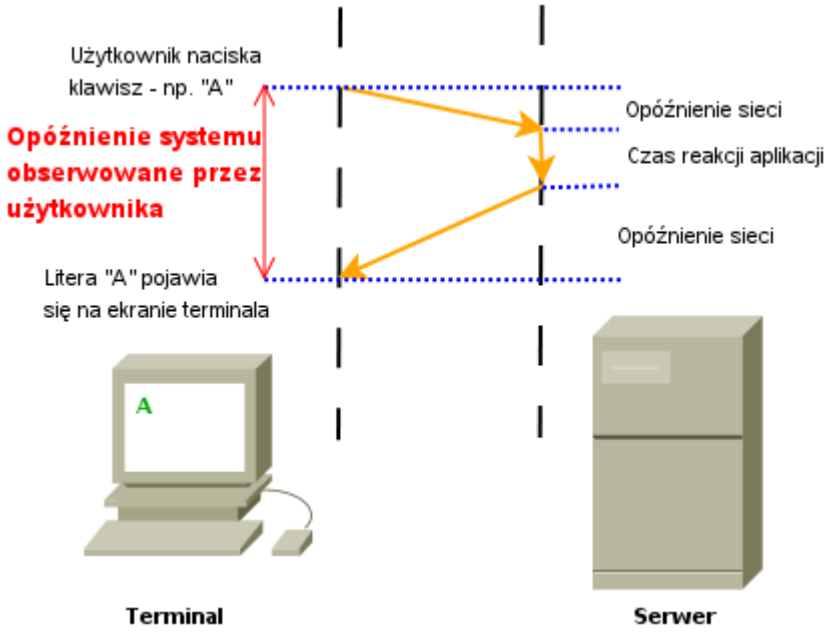
Wzrost wydajności i spadek cen popularnych komputerów, rozwiązania wieloprocesorowe i wielordzeniowe oraz wprowadzenie systemu MS Windows NT oraz praktyczne zastąpienie kosztownych systemów klasy UNIX przez licencjonowany nieodpłatnie system LINUX spowodowało zatrzymanie się wahadła i ponowne wprowadzenie rozwiązań terminalowych.



Rysunek 2
Uproszczona architektura terminalowa

Obecnie mamy do dyspozycji szereg protokołów do obsługi terminali sieciowych. Najpopularniejsze z nich to RDP, ICA, VNC, X Window. Pojawiają się także nowe rozwiązania firmowe – VMware View, PcoIP itp.

Rozwiązania terminalowe stawiają zupełnie inne wymagania przed sieciami komputerowymi. Najistotniejszym parametrem jest w tym przypadku opóźnienie transmisji na drodze klient-serwer-klient, a nie szybkość transmisji plikowych.



Rysunek 3
„Round trip delay” w pracy na terminalu

Powyższy rysunek dotyczy oczywiście transmisji w trybie tekstowym (np. pracy z edytorem). Transmisje strumieni (np. wyświetlanie filmu) są znacznie mniej czułe na opóźnienia, a wymagają odpowiedniego pasma sieciowego, jednak w pracy profesjonalnej (edycja dokumentów, wypełnianie formatek itp.) praca z tekstami jest najczęściej spotykana.

Jedną z największych zalet rozwiązania terminalowego jest brak składowania danych naic terminalu. Zwiększa to zasadniczo poziom ich bezpieczeństwa, ponieważ nie opuszczają one strefy zabezpieczonej fizycznie (serwerowni). Nawet kradzież terminala nie stanowi zagrożenia dla bezpieczeństwa danych, bo ich tam po prostu nie ma! Obniża to zasadniczo koszty eksploatacji system, nie ma bowiem potrzeby zabezpieczania terminali przed wirusami (nie wykonują one żadnych programów) oraz rozwiązywania problemów związanych z zarządzaniem kopiami awaryjnymi znacznej liczby komputerów osobistych. Nie trzeba więc inwestować w drogie licencje korporacyjne odpowiednich programów narzędziowych.

Wirtualizacja pulpitu (Desktop Virtualization)

Wirtualizacja pulpitu jest rozwiązaniem, które powinno połączyć zalety indywidualnego komputera PC oraz terminala (cienkiego klienta). Fizycznie przetwarzanie danych następuje nadal w strefie bezpiecznej – jednak użytkownik uzyskuje praktycznie takie same możliwości jak użytkownik komputera PC podłączonego do lokalnej sieci korporacyjnej. Jego stanowisko pracy umożliwia mu pełny dostęp do przydzielonej mu maszyny wirtualnej lub fizycznej, lecz zainstalowanej w bezpiecznej serwerowni.

Dostawcy sprzętu oferują rozwiązania specjalnie dostosowane do budowy tego środowiska – na przykład „Blade PC". Są to kasety, w których instalowane są karty pełniące funkcje klasycznego komputera PC (np. posiadają dysk twardy lub dysk półprzewodnikowy) z indywidualnym systemem operacyjnym.

Rysunek 4
Kaseta i komputer „Blade PC"

Wykorzystywanie Blade PC umożliwia przeniesienie całości przetwarzania danych do bezpiecznej serwerowni, znaczną oszczędność miejsca oraz zużycia energii elektrycznej. Ułatwiony jest także nadzór administracyjny nad pracą systemu. Niestety koszty budowy środowiska wirtualnego pulpitu w oparciu o Blade PC są początkowo dość wysokie.

Drugim rozwiązaniem jest skorzystanie z maszyn wirtualnych. Technologia wykorzystywana przy już dość powszechnie przy wirtualizacji serwerów może być z powodzeniem wykorzystana do tworzenia wirtualnych komputerów PC w systemie komputera-gospodarza i przydzielania tych wirtualnych maszyn poszczególnym użytkownikom do indywidualnego wykorzystywania. Rozwiązanie to wydaje się być bardziej ekonomiczne, lecz należy brać pod uwagę, że mogą wystąpić pewne trudności w przypadku dużej liczby systemów-gości związane z obsługą sieci.

Oczywiście nic nie stoi na przeszkodzie, aby do wirtualizacji pulpitu wykorzystywać klasyczne komputery PC, jednak to rozwiązanie należy traktować raczej jako tymczasowe.

Należy podkreślić, że środowisko wirtualnego pulpitu to może być utożsamiane ze środowiskiem terminalowym. Pomimo że z punktu widzenia użytkownika różnica może być prawie niewidoczna, to jednak w rozwiązaniu terminalowym mamy do czynienia z systemem wielodostępu do jednego, wieloużytkownikowego systemu operacyjnego i współdzieleniem jego zasobów.

Stanowiska pracy użytkowników

W rozwiązaniach VDI (Virtual Desktop Infrastructure) stanowisko pracy jest wykorzystywane jako sieciowe urządzenie wejścia i wyjścia. Powinno zapewnić ono użytkownikowi taki sam komfort pracy jaki zapewnia bezpośrednia praca na indywidualnym komputerze PC.

Cienki klient (terminal sieciowy)

Podstawowe cechy tego rozwiązania to brak możliwości lokalnego wykonywania jakichkolwiek programów oraz składowania jakichkolwiek danych. Cienki klient działa jedynie jako zdalna konsola systemu z możliwością obsługi podłączonych lokalnie urządzeń peryferyjnych. W wielu rozwiązaniach cienki klient jest w ogóle pozbawiony pamięci masowej (nie posiada twardego dysku ani dysku półprzewodnikowego) i pobiera swój system operacyjny z dedykowanego serwera sieciowego (system NetBOOT) – np. w środowisku PXE (Preboot eXucution Environment). Dostępne jest szereg rozwiązań realizujących taką funkcję – zarówno otwartych (projekt LTSP – Linux Terminal Server Project), jak i komercyjnych np. wyspecjalizowanej w takich rozwiązaniach firmy 2X: 2X ThinClientServer oraz 2X VirtualDesktopServer oferującej produkty przeznaczone do wykorzystywania w środowisku MS Windows.

Zaawansowane rozwiązania komercyjne umożliwiają korzystanie ze środowiska witualnego desktopu również w różnych środowiskach systemowych.

Rysunek 5
Wirtualny pulpit w systemach iPad, iPhone oraz Android

Sieciowa stacja robocza

Wiele firm (między innymi również firma ABA) oferuje terminale sieciowe, które powinny być właściwie określane mianem stacji sieciowej). Są one wyposażone w lokalny system operacyjny (ładowany najczęściej z pamięci FLASH), a więc uruchamiają się autonomicznie, bez potrzeby ładowania systemu operacyjnego z serwera. Takie urządzenia są również często wyposażane w lokalne programowanie – np. przeglądarkę WWW, klientów VoIP (mp. SKYPE), przeglądarki plików w formatch PDF, DjVU oraz dodatkowe protokoły komunikacyjne, systemy automatycznej konfiguracji itp. Można je traktować jako „pośrednie ogniwo" pomiędzy cienkimi klientami, a komputerami PC, jednak zazwyczaj ze względów bezpieczeństwa nie mogą one trwale przechowywać lokalnie danych (np. hstorii odwiedzanych stron oraz „ciasteczek"). Jako pamięć podręczna wykorzystywana jest przez użytkownika pamięć RAM (RAM dysk), a możliwość trwałego zapisu konfiguracji w pamięci FLASH jest rezerwowana dla administratora systemu.

Rozwiązanie to jest właściwie pośrednim pomiędzy prawdziwie cienkim klientem, a komputerem PC (system operacyjny takiego urządzenia to Embedded LINUX lub Embedded Windows), ponieważ oprócz pracy jako końcówka wirtualnego pulpitu lub terminal sieciowy może być wykorzystywana również jako autonomiczna stacja WWW – np. końcówka ABA-X3 jest wyposażana w pełną wersję przeglądarki Firefox z obsługą środowiska JAVA, Flash Player itp.

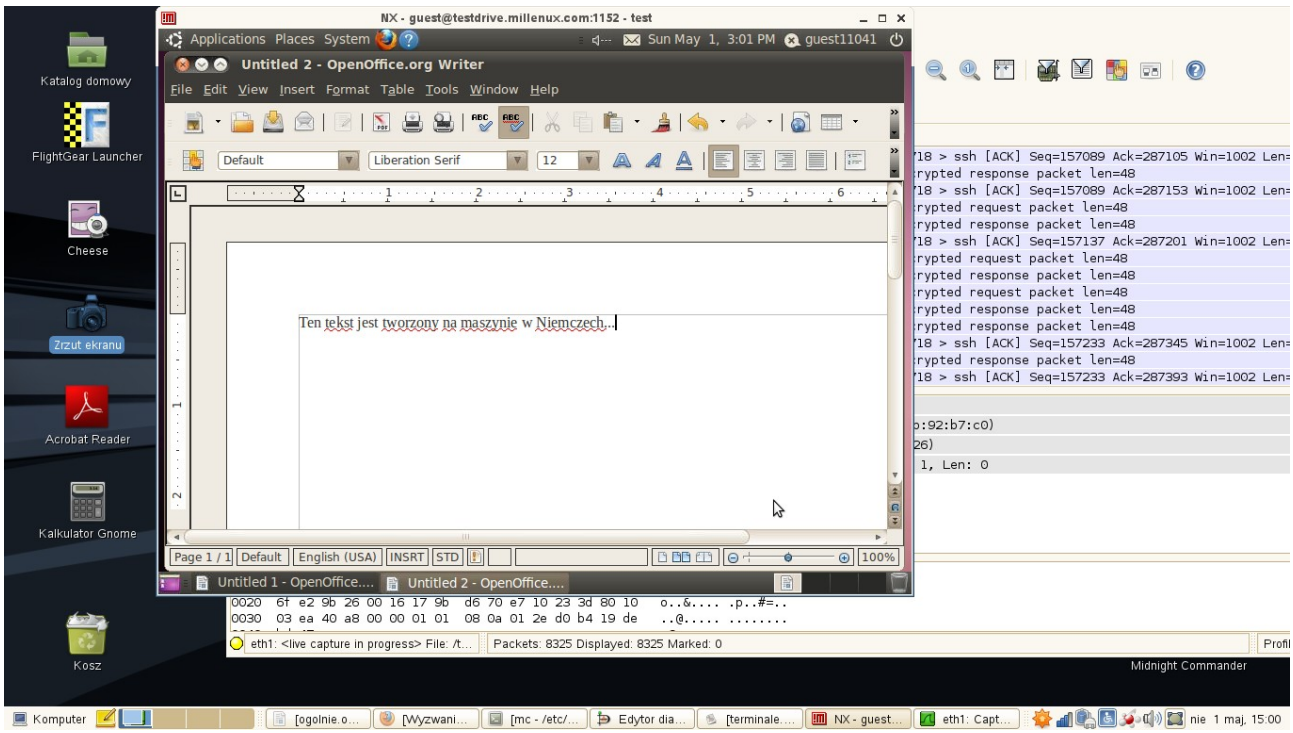
Komputer PC

Każdy komputer PC niezależnie od systemu operacyjnego może pełnić rolę terminala sieciowego lub końcówki wirtualnego desktopu. Musi zostać jednak wyposażony w oprogramowanie klienta wybranego protokołu komunikacyjnego. Właściwy wybór protokołu ma zasadnicze znaczenie dla powodzenia przedsięwzięcia.

Badania przeprowadzone na Politechnice Krakowskiej wykazały, że protokoły, które wymagają znacznego pasma sieciowego (transmitują dużo danych) charakteryzują się szybkimi odpowiedziami aplikacji (patrz rys. 3), zaś protokoły, które minimalizują transmisje sieciowe wprowadzają z kolei większe opóźnienia na serwerach. Wiąże się to oczywiście z ich rozbudowanymi funkcjami – np. z procesem kompresji danych. Tym niemniej umożliwiają one efektywne wykorzystywanie wirtualnego pulpitu nawet w stosunkowo wolnych sieciach rozległych.

Praca w sieci rozległej wiąże się oczywiście z koniecznością ochrony transmisji sieciowych co prowadzi do szyfrowania przesyłanych informacji. Operacja szyfrowania wiąże się z obciążeniem mocy obliczeniowej, co w konsekwencji prowadzi do dalszego zwiększania opóźnień w odpowiedzi aplikacji. Można zapobiec temu niekorzystnemu zjawisku wprowadzając maszyny pośredniczące – jak np. ABA IPSec Gateway lub nowsze ABA NX Gateway, które zostały dostosowane specjalnie do realizacji środowiska wirtualnego desktopu.

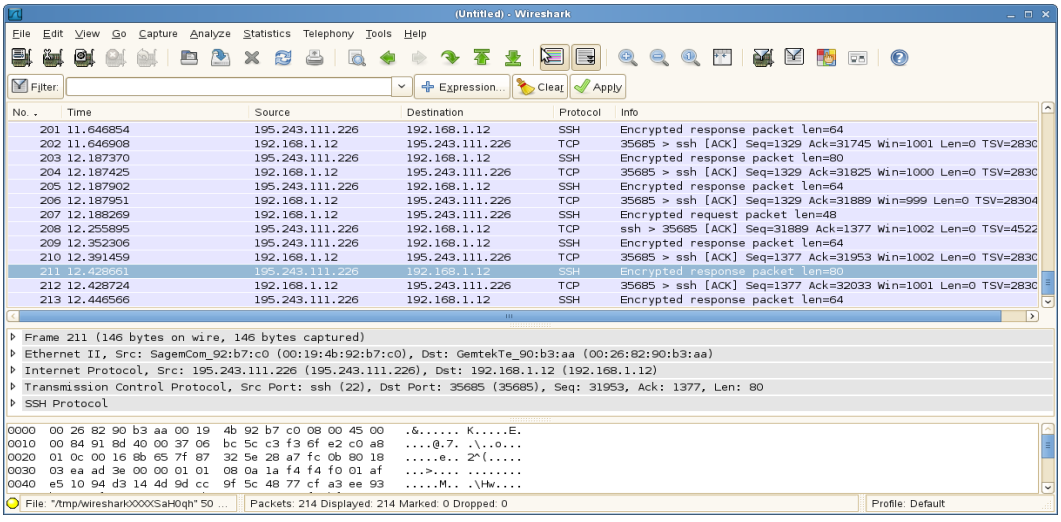
Oprogramowanie klient protokołu NX (nxclient) jest dostępne nieodpłatnie dla systemów LINUX (rpm, deb oraz tar), MS Windows, MacOS oraz Solaris. Podłączanie kolejnych stanowisk nie jest więc związane z dodatkowymi kosztami zakupu licencji.



Rysunek 6
Praca z programem Open Office w sieci Internet

Komputer, z którego pochodzi zrzut ekranu jest podłączony do Internetu za pomocą Neostrady przez urządzenie LiveBox i łącze o prędkości deklarowanej 2 Mbps/316 kbps. Średni czas ICMP Echo Requst (ping) do maszyny wirtualnej testdrive.millenux.com wynosi ok. 65 ms.

Całość transmisji jest oczywiście szyfrowana:

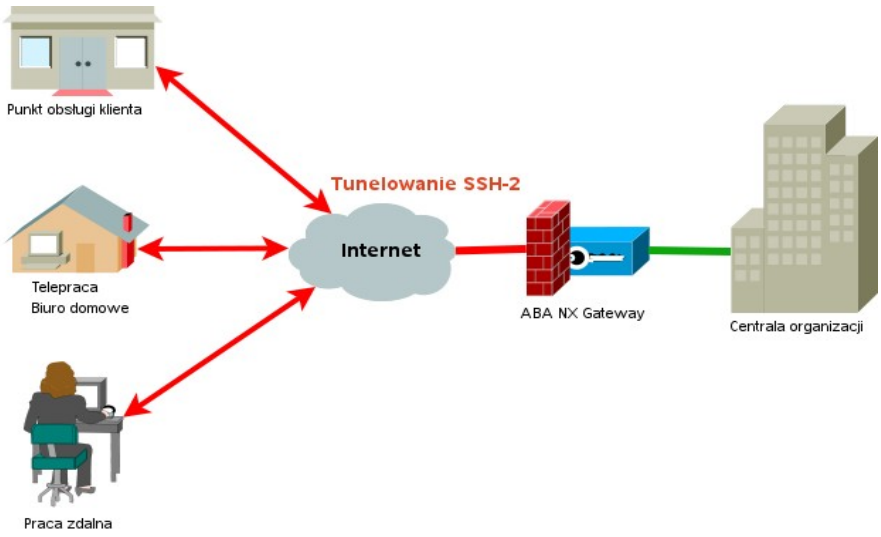


Rysunek 7
Analiza transmisji realizowanych przez protokół NX

Połączenie zrealizowane zostało przy użyciu protokołu NoMachine NX, który wykorzystuje do uwierzytelniania oraz szyfrowania transmisji mechanizmy SSH-2 oraz efektywną kompresję danych. Dzięki temu możliwe jest swobodne pisanie tekstu w edytorze Open Office.

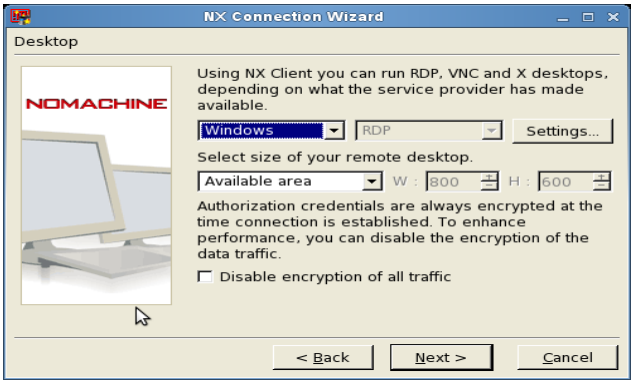
Wirtualizacja pulpitu i telepraca

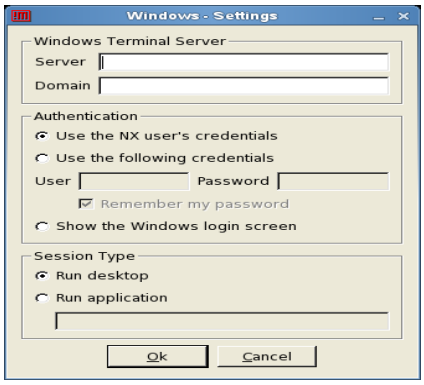
Technologia zdalnego wirtualnego pulpitu znakomicie nadaje się do pracy zdalnej. Obecnie dostęp do w miarę szybkiego (ok. 1 Mbps) łącza sieciowego nie stanowi już większego problemu. Podstawowa właściwość tej technologii, którą jest korzystanie jedynie ze zdalnych programów oraz brak konieczności transmisji danych na komputery pracujące poza bezpieczną siecią korporacyjną jest wręcz nie do przecenienia przy tworzeniu niewielkich zdalnych placówek, filii lub organizacji telepracy (Home Office):



Rysunek 8
Idea realizacji połączeń zdalnych za pomocą protokołu NX

Realizację bezpiecznych połączeń zdalnych znacznie ułatwia urządzenie ABA NX Gateway. Może ono pracować w trybie PROXY. Zdalni użytkownicy nawiązują połączenie z ABA NX Gateway w wyniku czego zostaje zestawiony bezpieczny tunel SSH. Następnie realizowane jest połączenie z serwerem w sieci lokalnej organizacji



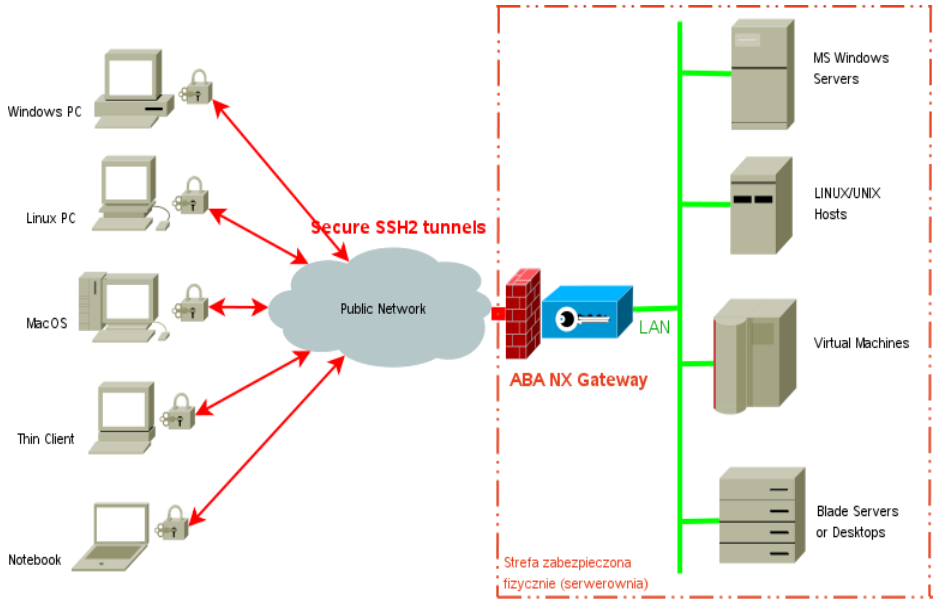


Może być to zarówno serwer usług terminalowych MS Windows (połączenie jest wówczas realizowane za pomocą klienta protokołu RDP lub ICA), host systemu UNIX lub LINUX (X11Rx), dowolny serwer VNC. Możliwe jest również wykorzystanie innych protokołów pod warunkiem zainstalowania odpowiedniego klienta na ABA NX Gateway (np. IBM 3270 lub 5250).

Istotną zaletą tego rozwiązania jest zastosowanie techniki proxy. Dzięki temu, że połączenia z serwerami dostępnymi w sieci lokalnej nawiązywane są *de-facto* przez klientów programowych zainstalowanych na ABA NX Gateway, a nie bezpośrednio przez urządzenia zdalne możliwe jest zastosowanie ścisłej filtracji pakietów na wejściu tego urządzenia (otwarty jest jedynie port 22 lub inny wybrany dla połączeń SSH) oraz uwierzytelnienia zdalnych klientów za pomocą algorytmu DSA jeszcze przed uzyskaniem jakiegokolwiek połączenia z siecią lokalną.

Połączenie z ABA NX Gateway wymaga odpowiedniego klienta programowego. Jest on udostępniany nieodpłatnie dla systemów rodzin MS Windows, Linux (w wersjach rpm, deb oraz tar) oraz UNIX (Solaris). Umożliwia to korzystanie z wirtualnego pulpitu użytkownikom nieomal każdego popularnego systemu – np. użytkownikom MS Windows z pulpitu maszyn Linuxowych lub odwrotnie – użytkownikom Linuksa ze zdalnego pulpitu MS Windows.

Również terminale sieciowe oraz ich oprogramowanie oferowane przez firmę ABA są dostarczane z klientami protokołu NX (ABA-X3 oraz 2X ThinClientServer). Firma ABA jest oficjalnym partnerem VAR firmy NoMachine, co uprawnia nas do wykorzystywania oprogramowania tej firmy w naszych autorskich rozwiązaniach oraz oczywiście do jej sprzedaży produktów.



Rysunek 9
Uproszczony schemat połączeń stanowisk zdalnych z siecią lokalną organizacji

Proszę zauważyć, że tak naprawdę zdalni użytkownicy pracują w sieci lokalnej – ABA NX Gateway przekazuje na zewnątrz jedynie obrazy ekranów i przyjmuje polecenia (naciśnięcie klawisza, ruch myszki itp.). Wszelkie transmisje zewnętrzne są szyfrowane (patrz rys. 7), a więc zagrożenie podsłuchem lub przejęciem sesji jest bardzo niewielkie.

Dzięki poczwórnemu zabezpieczeniu (filtracja pakietów dopuszczająca ruch tylko na jednym wybranym dla SSH porcie, obustronne uwierzytelnienie zdalnej stacji algorytmem DSA, szyfrowanie transmisji oraz zastosowanie proxy) użytkownicy zdalnych pulpitów mogą otrzymać takie same uprawnienia, jak użytkownicy pracujący w sieci lokalnej w siedzibie organizacji. Możliwe jest także przenoszenie sesji pomiędzy stanowiskami sieciowymi – użytkownik może odłączyć się od sesji, która pozostanie jednak aktywna. Do sesji można się ponownie podłączyć z innego stanowiska – możliwe jest także podłączenie się do sesji nawiązanej ze zdalnego pulpitu ze stanowiska pracy w sieci lokalnej lub odwrotnie. Możliwe jest także podłączenie się do aktywnej sesji na komputerze PC użytkownika.c

Praktyczna realizacja systemu:

System wykorzystuje oprogramowanie firmy NoMachine (NX). Polski Partner VAR – ABA zapewnia Państwu:

- Konsultacje techniczne przy projektowaniu i uruchamianiu systemu,
- Dostawę kompletnych urządzeń wyposażonych w odpowiednie oprogramowanie:
  - terminale sieciowe przeznaczone do uruchamiania sieciowego PXE (NetBoot),
  - oprogramowanie do ładowania systemu operacyjnego terminali oraz zarządzania nimi (dla serwerów MS Windows oraz Linux),
- Autonomicznie uruchamiane terminale ABA-X3 z modularnym oprogramowaniem systemowym konfigurowanym według indywidualnych wymagań zamawiającego,
- Kompletne, gotowe do pracy urządzenia ABA NX Gateway w wersjach Small Business (obsługa do 10 połączeń), oraz Enterprise (bez ograniczenia liczby użytkowników) oraz Advanced (dla systemów klastrowych z równoważeniem obciążenia),
- Komplet oprogramowania do samodzielnej budowy systemu wraz z opieką techniczną świadczoną bezpośrednio przez (roczne subskrypcje z gwarancją czasu odpowiedzi na zgłaszane problemy),
- Oprogramowanie narzędziowe do kontroli pracy sieci, wydajności aplikacji sieciowych oraz monitorowania połączeń – Network Instruments OBSERVER,
- Nieodpłatne wersje próbne z ograniczeniem liczby użytkowników.

Zestawienie właściwości technicznych wersji oprogramowania znajduje się na stronie naszej firmy: http://www.aba.krakow.pl oraz naszych partnerów:
NoMachine: http://www.nomachine.com/features.php,
2X Software: http://www.2x.com,
Novell: http://www.novell.com/poland/,
Network Instruments: http://www.networkinstruments.com,

Opisane powyżej rozwiązania wykorzystujemy w naszej sieci do codziennej pracy. Dzięki ich stosowaniu z każdego stanowiska pracy – lokalnego lub zdalnego możemy korzystać z wirtualnych pulpitów systemów MS Windows lub LINUX. Uważamy, że jest to najlepsza możliwa rekomendacja.