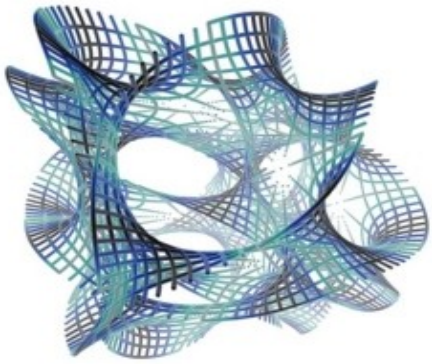
Old Man GURU Magazine

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

Wydanie specjalne 11/2011 9 Maj 2011

Virtual Desktop Infrastructure

Bezpieczny tunel do świata swobodnego wyboru (część druga)



Spis treści:

Zainteresowanie, z jakim spotkał się poprzedni, 10 numer OLD MAN GURU zainspirował mnie do napisania jego dalszego ciągu – tym razem poświęconego opisowi praktycznej instalacji rozwiązania wykorzystującego architekturę wirtualnego pulpitu (Virtual Desktop Infrastructure).

Opisywane rozwiązanie jest wykorzystywane przeze mnie w praktyce i umożliwia zdalne wykorzystywanie komputerów zainstalowanych w naszej firmie. Umożliwia ono w pełni efektywne i bezpieczne korzystanie z dowolnych komputerów zainstalowanych w sieci firmowej. Rozwiązanie pracuje w następującej konfiguracji dostępu do Internetu:

Firma dysponuje 8 własnymi adresami IP – jeden z nich przeznaczono wyłącznie do realizacji zdalnego dostępu za pomocą ABA NX Gateway. Udostępniane są zarówno komputery wykorzystujące system MS Windows, jak i system LINUX. Komputery te mają adresy sieciowe w podsieci 10.1.1.x .

Zdalny dostęp jest realizowany głównie za pośrednictwem popularnej Neostrady (lub innych podobnych rozwiązań), a więc komputery i terminale dostępowe posiadają adresy IP z sieci 192.168.x.x przydzielane przez DHCP. Połączenie z Internetem realizuje ruter wypożyczany przez dostawcę usług (w przypadku Neostrady TP S.A.). Dostęp zdalny jest możliwy zarówno z komputerów pracujących pod systemem LINUX, jak i Windows.

Instalacja oprogramowania

Pierwszym krokiem jest przygotowanie komputera, na którym będzie pracować ABA NX Gateway. Zasoby tej maszyny powinny być dostosowane do liczby równocześnie realizowanych połączeń. Powinna ona posiadać dwa interfejsy sieciowe, z których jeden zostanie wykorzystany do przyjmowania połączeń zewnętrznych, zaś drugi do połączenia z siecią lokalną.

Jeśli zamierzamy wykorzystywać ABA NX Gateway jako maszynę pośredniczącą w dostępnie do komputerów (desktopów lub serwerów) w sieci LAN nie musimy jej wyposażać w twardy dysk – wystarczy pamięć flash (np. DiskOnModule). W opisywanej instalacji użyto takiej pamięci o pojemności 4 GB. Należy jednak brać pod uwagę, że jednym z zadań ABA NX Gateway jest przygotowanie graficznego środowiska pracy dla użytkowników oraz szyfrowanie transmisji – konieczna więc będzie odpowiednia do potrzeb moc procesora oraz wielkość pamięci RAM.

Na przygotowanej maszynie instalujemy system operacyjny Linux (jedynie te składniki wybranej dystrybucji, które będą nam niezbędne). W opisywanej instalacji jest to openSuSE Linux. Konfigurując system zwracamy uwagę na to, aby prawidłowo skonfigurować połączenia sieciowe nie tworząc połączenia pomiędzy nimi. Można to sprawdzić za pomocą polecenia netstat -r . Ze względu na możliwe późniejsze utrudnienia w konfiguracji korzystne jest stosowanie statycznych adresów IP.

Kolejnym krokiem jest zainstalowanie zestawu oprogramowania NoMachine NX. Zestaw ten należy pobrać ze strony www.nomachine.com . Jeśli wystarczy nam wersja dla 2 równoczesnych połączeń, możemy wybrać nieodpłatną wersję NX Free. Jeśli planujemy realizować więcej połączeń, pobieramy wersję próbną (na 30 dni). Po wypróbowaniu będziemy mogli zakupić licencję wraz z subskrypcją w wersji, która nam odpowiada. Należy zwrócić uwagę, że oprogramowanie dla ABA NX Gateway musi zawierać moduł nxserver, a więc nie może być to wersja NX Desktop. Cena licencji jest uzależniona od liczby procesorów oraz od poziomu wsparcia technicznego, a nie od liczby połączeń. Wyjątkiem jest wersja Small Business, która zawiera ograniczenie umożliwiające zestawienie jedynie 10 równoczesnych połączeń.

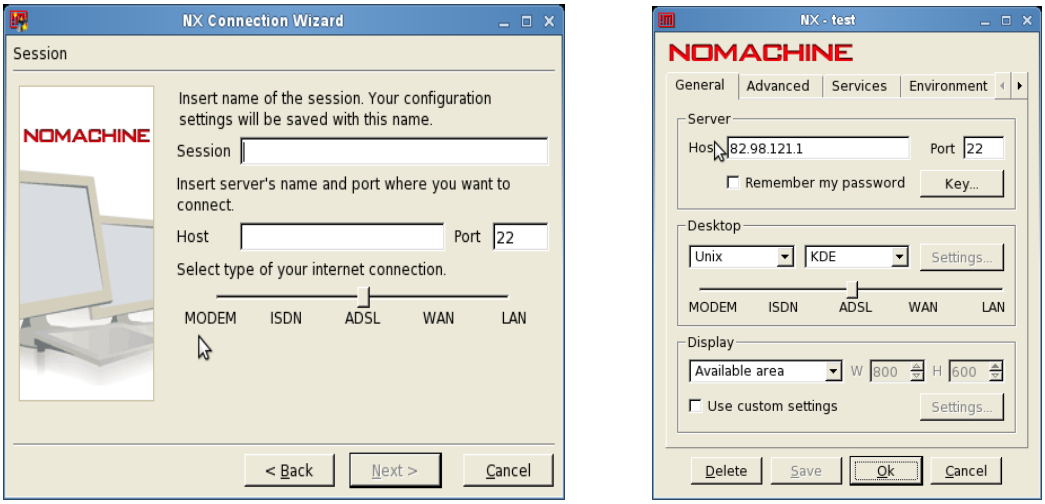
Następnie wprowadzamy odpowiednie zabezpieczenia połączeń sieciowych. Interfejs zewnętrzny powinien dopuszczać jedynie połączenia SSH. Możemy pozostawić dla nich standardowy port 22 lub zastosować inny. Poprawność konfiguracji powinniśmy sprawdzić za pomocą dowolnego skanera internetowego – np. nmap. Zabezpieczenie interfejsu realizującego połączenia zewnętrzne ma zasadnicze znaczenie dla bezpieczeństwa realizowanych połączeń zdalnych. Nie ma powodu, aby pozostawiać otwarte usługi (np. ICMP echo – ping) ponieważ każda zbędna funkcja może potencjalnie zostać wykorzystana do ataku sieciowego.

```
PORT   STATE SERVICE
22/tcp open  ssh
```

Celowe jest również ograniczenie usług dostępnych na interfejsie sieciowym podłączanym do sieci lokalnej. Konfiguracja filtracji dla tego interfejsu jest zależna od tego, jakie usługi (RDP, SSH, X Window itp.) zamierzamy udostępnić użytkownikom zewnętrznym. Głównym celem filtracji jest zapobieżenie możliwości wprowadzenia zmian w konfiguracji ABA NX Gateway przez użytkowników sieci wewnętrznej.

Kolejnym etapem jest instalacja oraz konfiguracja programów, które będzie wykorzystywać system ABA NX Gateway do połączeń z komputerami sieci lokalnej – na przykład klienta RDP (do połączeń z komputerami MS Windows), X Window lub SSH (do połączeń z maszynami Linux/Unix), VNC (zdalny bufor kadru) itp. ABA NX Gateway będzie realizować tylko te połączenia, dla których dysponuje odpowiednim klientem programowym.

Po skonfigurowaniu i sprawdzeniu poprawności obsługi sieci przez ABA NX Gateway możemy przystąpić do instalacji klientów programowych NX. Oprogramowanie NX Client jest dostępne nieodpłatnie dla systemów operacyjnych MS Windows, Linux (wersje rpm, deb oraz tar), MacOS oraz Solaris w wersjach 32 i 64 bitowej. Do konfiguracji klienta NX służy specjalny program graficzny – Connection Wizzard.



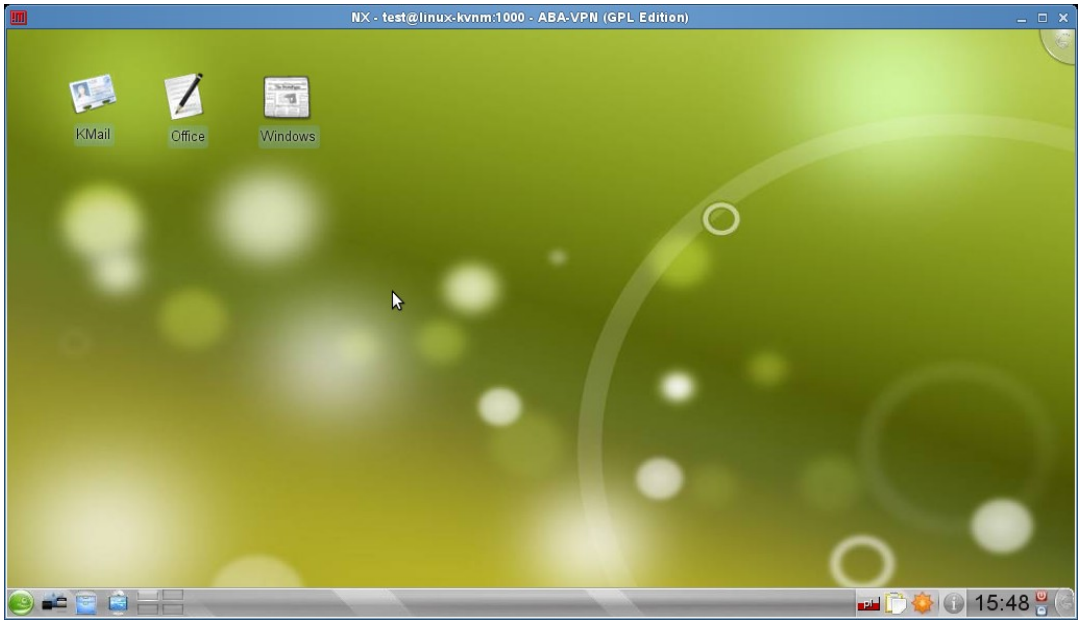
Rys.1
Program instalacyjny NX Wizzard

Program konfiguracyjny zapisuje parametry sesji w pliku konfiguracyjnym <nazwa_sesji>.nxs. W pliku tym znajdują się także klucze wykorzystywane w celu uwierzytelnienia klienta.

Połączenie klienta z serwerem NX jest realizowane w 2 etapach. Najpierw następuje uwierzytelnienie klienta. Służy do tego pomocniczy użytkownik o nazwie nx. Nie jest on klasycznym uniksowym „pseudouserem", ponieważ uruchamia proces /usr/bin/nxserver jako swoją „powłokę". Nie posiada hasła i jest wykorzystywany do zestawienia uwierzytelnionego za pomocą techniki kluczy prywatno-publicznych połączenia klienta z serwerem. Przekazanie danych użytkownika (login, hasło) następuje dopiero po uwierzytelnieniu stacji klienta już z wykorzystaniem połączenia szyfrowanego.

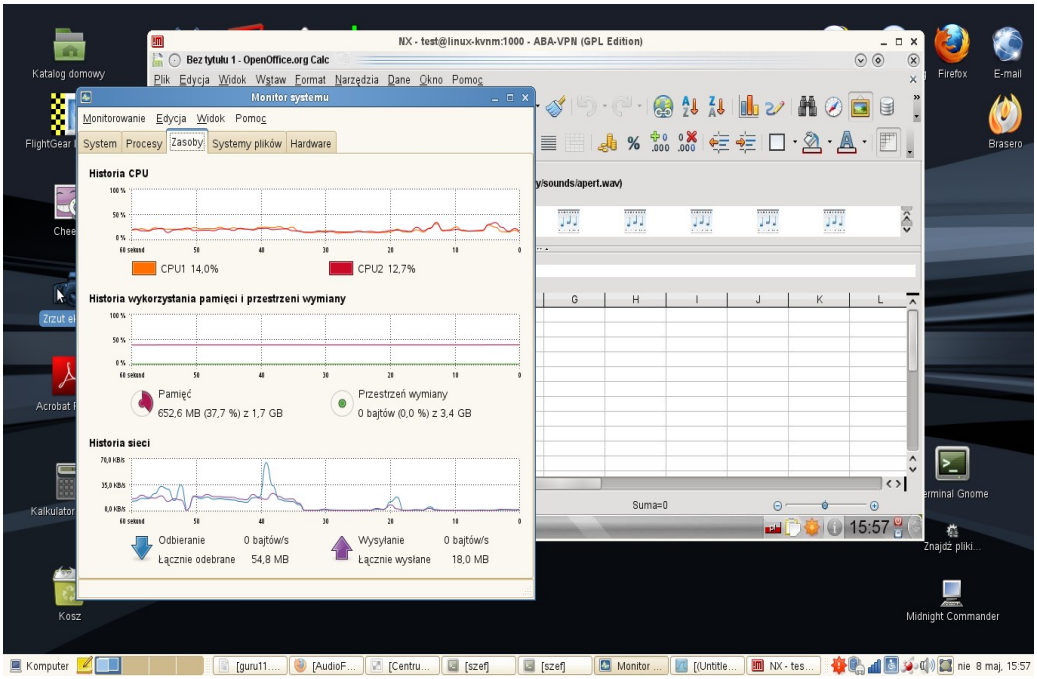
Kolejnym etapem jest uruchomienie programów komunikacyjnych użytkownika. Służą one realizowaniu połączeń z konkretnymi komputerami i programami użytkowymi. Skrypty startowe mogą być uruchamiane automatycznie albo poprzez wybór ikony (tak jak na załączonym przykładach):

```
ssh -X tomekb@10.1.1.231 thunderbird (ikona poczty elektronicznej)
ssh -X tomekb@10.1.1.241 soffice (ikona programu biurowego)
rdesktop -kpl 10.1.1.221 (ikona windows)
```

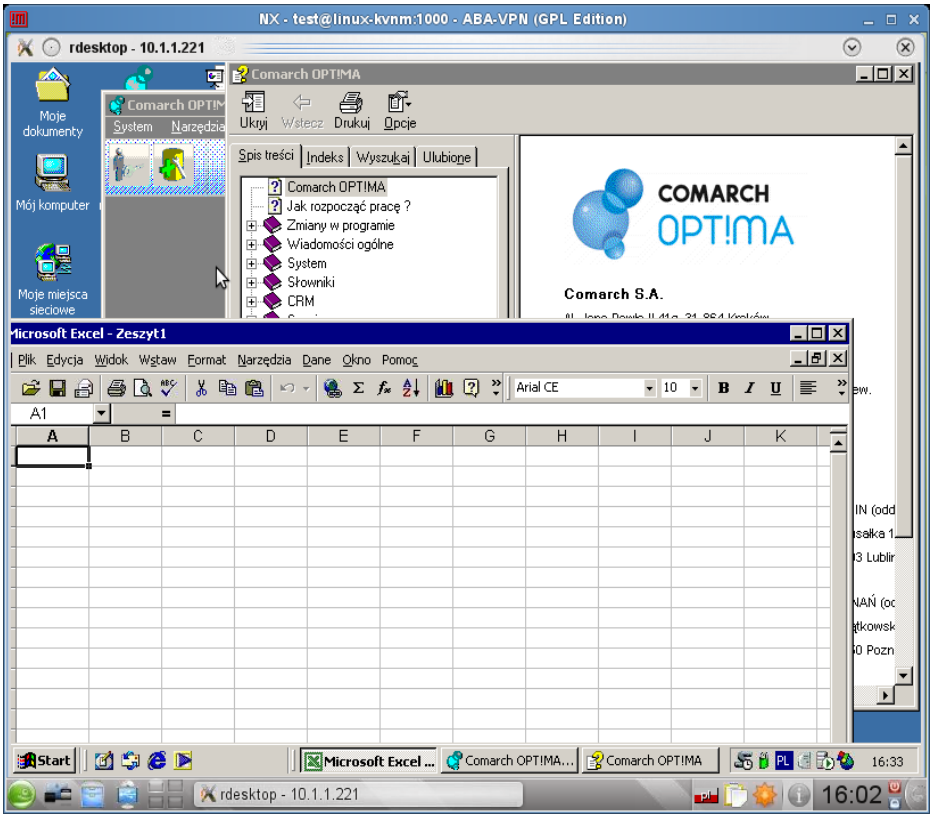


Rys.2
Ekran pulpitu realizującego dostęp do usług sieci organizacji

Na powyższym ekranie pokazano trzy ikony – dwie z nich uruchamiają programy użytkowe – klienta poczty elektronicznej oraz program OpenOffice. Trzecia umożliwia wykorzystywanie komputera MS Windows w trybie dostępu do pełnego pulpitu.

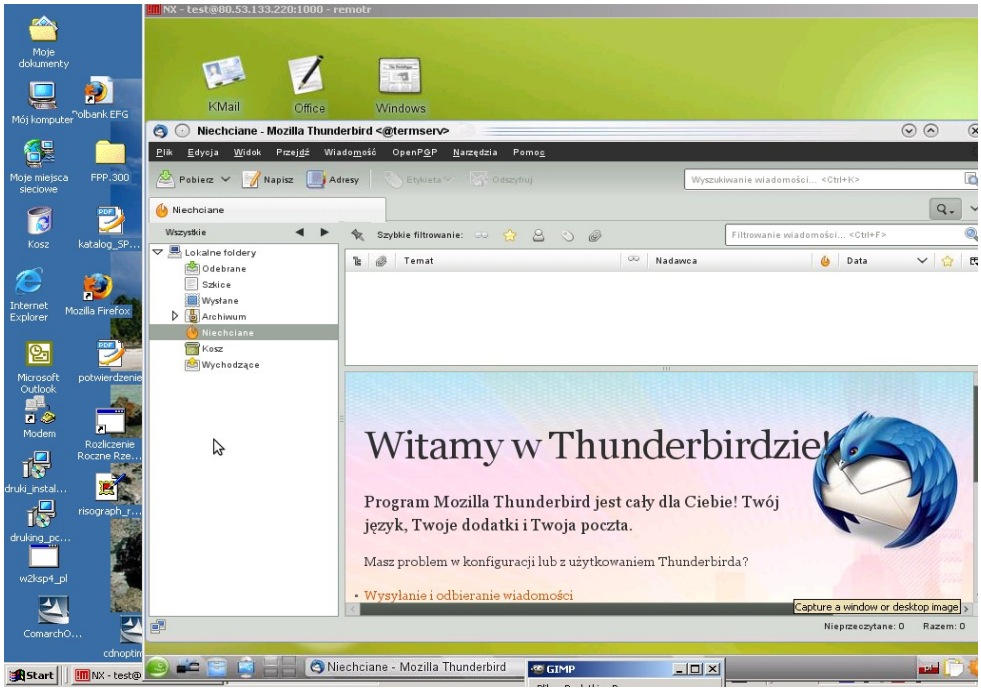


Rys.3
Praca ze zdalnym Open Office – proszę zwrócić uwagę na oszczędne wykorzystywanie pasma sieciowego!



Rys.4

Zdalny pulpit systemu Windows udostępniany na końcówce (Linux) Neostrady 1Mbps



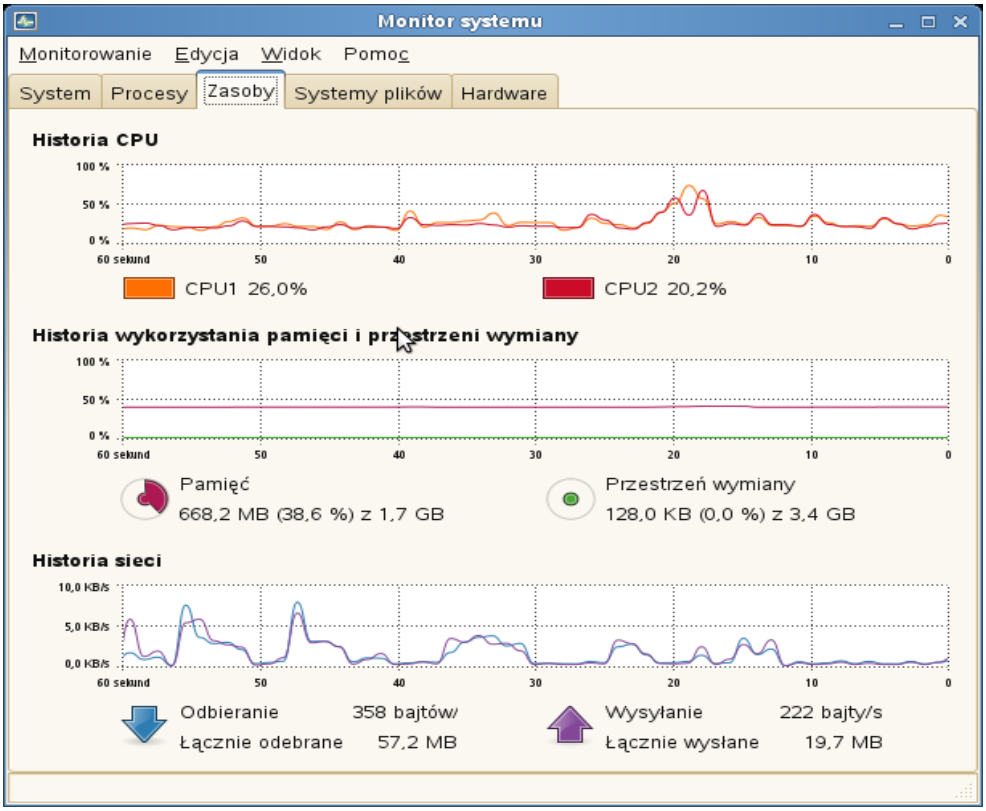
Rys. 5

Zdalny dostęp do sieci firmowej z komputera MS Windows

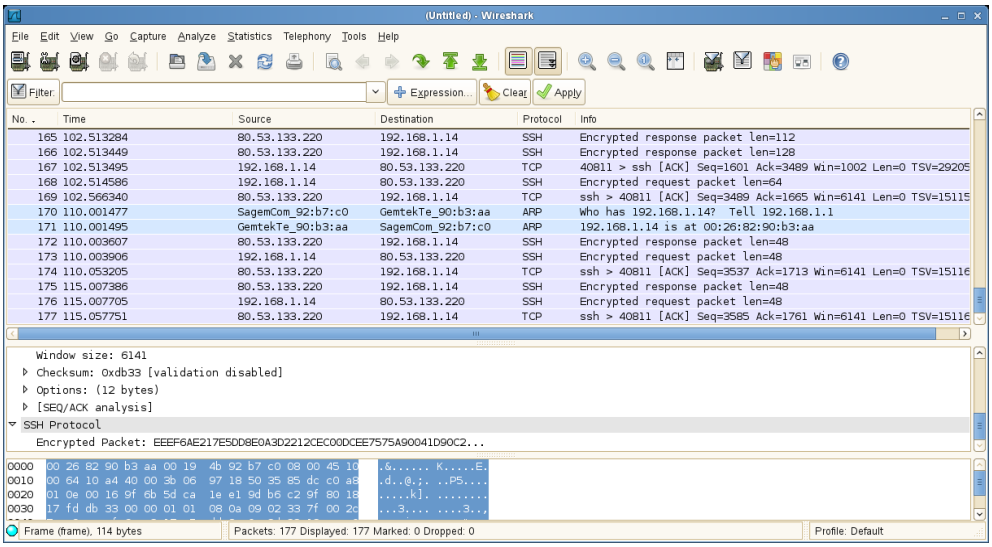
Funkcjonalność, jaką będzie dysponował użytkownik, zależy od konfiguracji jego środowiska, którą określa administrator. W najprostszym przypadku po pomyślnym uwierzytelnieniu użytkownik będzie dysponować pełnym dostępem do wybranego komputera w sieci lokalnej. Praca nie będzie się wówczas różnić od pracy na tym komputerze w sieci lokalnej. Wszystkie dane pozostaną w siedzibie firmy, ponieważ stacja robocza służy jedynie jako terminal graficzny.

Możliwe jest również korzystanie z programów pracujących na różnych serwerach aplikacji, niezależnie od systemu operacyjnego. Pozwala to na optymalizację kosztów licencji oprogramowania, ponieważ użytkownik może na jednym stanowisku korzystać zarówno w oprogramowania dla systemu MS Windows oraz LINUX. Programy te mogą korzystać ze wspólnego obszaru składowania danych (Network Attached Storage).

Takie rozwiązanie idealnie odpowiada potrzebom telepracy, ponieważ w pełni zabezpiecza dane firmowe, a telepracownik może realizować takie same zadania, jak osoba pracująca na komputerze w sieci lokalnej (bo przecież właśnie na takim komputerze w rzeczywistości pracuje).



Rys.6
Wykorzystywanie pasma transmisyjnego podczas pracy z arkuszem kalkulacyjnym.



Rys.7
Zestawienie transmitowanych pakietów sieciowych – proszę zwrócić uwagę na szyfrowanie transmisji.

Proszę zwrócić uwagę na to, jak niewielkie pasmo sieciowe jest wykorzystywane podczas pracy zdalnej. W trakcie wypełnienia arkusza kalkulacyjnego lub korzystania podczas edycji dokumentu wykorzystanie pasma sieciowego nie przekracza 10 kB/s. Większe obciążenia występują podczas uruchamiania programu (wymaga to wyświetlenia nowego okna z wieloma elementami), lecz i wówczas nie przekracza kilkudziesięciu kilobajtów na sekundę.

Firma ABA dostarcza nie tylko oprogramowanie firmy NoMachine, lecz również proponuje Państwu kompletne urządzenia „Network Appliance” ABA NX Gateway oraz specjalizowane wyposażone w klienta programowego NX.

W połączeniu z oprogramowaniem firmy 2X (www.2x.com), które jest przeznaczone do zarządzania publikowaniem aplikacji oraz zarządzania oprogramowaniem końcówek sieciowych, produktami firmy NOVELL jesteśmy w stanie zaproponować Państwu kompletne rozwiązanie. Jak zapewne zdołałem już Państwa przekonać, jest ona dostosowane do współpracy z obecnie wykorzystywanymi systemami komputerowymi.

Przykłady zastosowań

Bezpieczny wirtualny pulpit w sieci lokalnej

Często spotykamy się z następującym problemem: W dużej sieci lokalnej organizacji część pracowników wykonuje zadania wymagające przetwarzania danych kwalifikowanych (dane osobowe, wrażliwe, informacje będące istotnymi aktywami organizacji itp.). Ze względów bezpieczeństwa komputery, na których składowane są te dane, powinny być zabezpieczone fizycznie. Konieczne jest również odpowiednie zabezpieczenie transmisji sieciowych realizowanych przez sieć lokalną wykorzystywaną do innych celów.

Problem ten można łatwo rozwiązać przenosząc komputery PC (bez monitorów) wykorzystywane do przetwarzania tych danych do strefy zabezpieczonej fizycznie (np. do serwerowni), w której również umieszczamy urządzenie ABA NX Gateway. Użytkownicy będą korzystać z tych maszyn zdalnie, korzystając z prostych, bezdyskowych końcówek (terminali) wyposażonych w klienta programowego NX (nxclient) 2X ThinClientServer. Na końcówkach tych nie można składować żadnych danych, co powoduje, że pomieszczenia, w których są one wykorzystywane, nie muszą być starannie fizycznie zabezpieczane – nawet poza godzinami służbowymi. Wyłączenie możliwości komunikacji (np. urządzenia dostępowego ABA NX Gateway) po zakończeniu pracy uniemożliwia jakikolwiek dostęp do danych z tych pomieszczeń.

Taki sposób pracy nie tylko zapewnia, że dane będą składowane na dyskach komputerów umieszczonych w strefie bezpiecznej, lecz gwarantuje także poufność transmisji sieciowych (są one szyfrowane) oraz pełną kontrolę dostępu (niezależne uwierzytelnienie stacji roboczej i użytkownika). Realizowane połączenia mogą być zapisywane w odpowiednich dziennikach systemowych ABA NX Gateway, co zapewnia właściwy poziom Systemu Zarządzania Bezpieczeństwem Informacji (SZBI) oraz ułatwia wypełnienie warunków normy ISO/IEC 27001.

Należy podkreślić, że wykorzystanie tego rozwiązania w żaden sposób nie ogranicza komfortu pracy użytkowników, ponieważ w dalszym ciągu dysponują oni pełnymi możliwościami swych komputerów PC, a jedynie obsługują je zdalnie, wykorzystując środowisko wirtualnego desktopu (VDI – Virtual Desktop Infrastructure).

Zdalny punkt obsługi klienta lub mała filia:

Pomimo rozwoju różnego rodzaju e-usług w wielu przypadkach niezbędna jest bezpośrednia obsługa klienta w pobliżu jego miejsca zamieszkania lub w miejscu, gdzie przebywa sporo osób (centra handlowe, dworce, atrakcje turystyczne itp.).

Powodzenie biznesowe takiego punktu obsługi klienta (POK) zależy od wielu czynników, ale jednym z najważniejszych jest zakres świadczonych przez niego usług. Konieczne jest również zapewnienie odpowiedniego poziomu bezpieczeństwa danych – także w czasie, gdy POK jest nieczynny.

Rozwiązanie wirtualnego pulpitu (VDI) spełnia idealnie te wymagania, ponieważ:

- Zakres świadczonych usług może być taki sam jak w placówce macierzystej. Pracownicy obsługujący POK w rzeczywistości pracują bowiem na komputerach zainstalowanych w centrali i podłączonych do jej sieci lokalnej.
- Zastosowanie końcówek bezdyskowych powoduje, że w POK nie są gromadzone żadne dane w postaci elektronicznej – natomiast pracownik dysponuje pełnym dostępem do wszystkich niezbędnych mu danych oraz programów – w taki sam sposób, jak pracownik w sieci lokalnej centrali.
- Połączenia sieciowe POK są możliwe dopiero po pełnym uwierzytelnieniu stacji roboczej (końcówki) przy wykorzystaniu systemu kluczy prywatnych i publicznych. Wyklucza to w praktyce możliwość podłączenia się do systemu przez inną, nieuprawnioną końcówkę. Dopiero po uwierzytelnieniu końcówki użytkownik może podać swoje osobiste dane uwierzytelniające („login" i hasło). Ich transmisja jest już realizowana poprzez zestawiony kanał szyfrowany końcówka – urządzenie dostępowe ABA NX Gateway.
- Pracownicy POK mogą korzystać z zestawionego szyfrowanego kanału komunikacyjnego do przesyłania wydruków dokumentów na drukarki umieszczone w POK oraz również do bezpiecznej komunikacji głosowej (VoIP).

System obsługi zdalnych POK oparty o zdalną pracę placówek terenowych został wdrożony między innymi przez kilka banków w Polsce. Sprawdza się również znakomicie w rozwiązaniach obsługi zdalnej sprzedaży. Znakomitym uzupełnieniem systemu po stronie centrali jest oprogramowanie przeznaczone do udostępniania aplikacji – 2X AppliacationServer for Windows Terminal Services.

Telepraca

W Polsce telepraca jest uregulowana ustawowo, lecz jak dotychczas nie zdobyła większej popularności. Moim zdaniem jest to spowodowane przede wszystkim tym, że telepraca jest postrzegana jako niewygodna forma samozatrudnienia. Tymczasem telepracownik może być efektywny tylko wówczas, gdy będzie dysponował takimi samymi możliwościami, jak pracownik posiadający własne biurko w firmie.

Telepraca nie jest synonimem pracy mobilnej – najczęściej jest wręcz przeciwnie, telepracownik dysponuje stanowiskiem pracy, które nie jest zlokalizowane w siedzibie firmy – może to być na przykład biurko w jego mieszkaniu.

Telepraca jest korzystna dla obu stron – pracodawcy i pracobiorcy. Dla pracodawcy oznacza zmniejszenie kosztów stałych, zaś dla pracobiorcy znaczną oszczędność czasu (dojazdy, które stają się coraz bardziej uciążliwe) oraz w wielu przypadkach znaczną wygodę. Telepraca jest wręcz idealnym rozwiązaniem, które umożliwia utrzymanie aktywności zawodowej kobiet w wieku rozrodczym, aktywizację osób starszych, których doświadczenie jest często znakomitym uzupełnieniem „młodych, dynamicznych zespołów" itp.

System telepracy musi jednak być bezpieczny (informacje istotne dla pracodawcy muszą pozostawać pod jego kontrolą) oraz efektywny (telepracownik musi mieć pełną możliwość wykonywania zadań wynikających z potrzeb biznesowych firmy lub organizacji). Właśnie takie właściwości zapewnia opisany powyżej system.

Co równie ważne telepracownik otrzymuje od pracodawcy specjalną bezdyskową końcówkę (terminal) skonfigurowaną w sposób umożliwiający połączenie z komputerami zainstalowanymi w głównej siedzibie firmy lub organizacji. Nie może być ona wykorzystywana w innych celach oraz zawiera odpowiednie klucze autoryzacji umożliwiające połączenie z urządzeniem dostępowym firmy. Nie ma więc obawy, że na stanowisku pracy telepracownika będą instalowane przez niego jakiekolwiek programy, zapisywane dane niewiadomego pochodzenia (np. zdjęcia wymieniane z przyjaciółmi), które mogą być nośnikami wirusów i innych złośliwych programów – bo po prostu jest to niemożliwe. Podobnie – poczta elektroniczna telepracownika cały czas pozostaje na serwerze firmy w jej głównej siedzibie.

Nie ma więc potrzeby budowy drogiego systemu tworzenia (i odtwarzania) kopii awaryjnych komputerów telepracowników, instalacji na nich oprogramowania antywirusowego itp. itd. W przypadku uszkodzenia końcówki jest ona po prostu wymieniana na sprawną po wprowadzeniu (w ciągu kilku minut) odpowiednich danych konfiguracyjnych i kluczy uwierzytelniających.

Oczywiście możliwe jest także wykorzystanie komputera PC jako stanowiska telepracy (z systemem MS Windows, Linux lub MacOS), jednak należy wówczas zadbać o jego odpowiednie zabezpieczenie, co podnosi znacząco koszty rozwiązania.