
Skrócona instrukcja obsługi systemu VPN w Szkole Głównej Handlowej w Warszawie

Wprowadzenie

VPN to skrót od nazwy Virtual Personal Network (*Wirtualna Sieć Prywatna*) umożliwiająca połączenie komputera znajdującego się fizycznie poza kampusem SGH do sieci lokalnej SGH w sposób bezpieczny za pośrednictwem szyfrowanego kanału transmisji. Po połączeniu komputera do usługi VPN następuje logiczne „przeniesienie” komputera do lokalnej sieci SGH, tak jakby komputer znajdował się fizycznie na terenie SGH. VPN zapewnia dostęp do wielu usług, z których dziś można korzystać tylko i wyłącznie na miejscu w SGH.

Aktualnie zgodnie z informacją otrzymaną z Biblioteki SGH, system VPN pozwala na zdalny dostęp do następujących zasobów:

- ScienceDirect: <http://www.sgh.waw.pl/ogolnuczelniane/biblioteka/bazy/ScienceDirect/>
- SpringerLink: <http://www.sgh.waw.pl/ogolnuczelniane/biblioteka/bazy/springerlink/>
- Bazy danych : <http://www.sgh.waw.pl/ogolnuczelniane/biblioteka/bazy/>
(dotyczy tylko tych, które w kolumnie "sposób dostępu" zaznaczone są pomarańczowym kolorem)
- Czasopisma dostępne on-line:
<http://www.sgh.waw.pl/ogolnuczelniane/biblioteka/zbiory/coo-line/>
- Czasopisma od A do Z: <http://www.sgh.waw.pl/ogolnuczelniane/biblioteka/zbiory/Czasopisma%20od%20A%20do%20Z/>
- Laureaci nagrody Nobla: <http://www.sgh.waw.pl/ogolnuczelniane/biblioteka/nobel/>

Poza systemami wskazanymi przez Bibliotekę, VPN umożliwi pracę w systemie WorkFlowGen oraz pracę z innymi systemami w oparciu o zdalny pulpit lub terminal tekstowy, pod warunkiem, że pozwala na to licencja lub warunki umowy na korzystanie z danego oprogramowania/systemu.

Zgodnie z zapewnieniem producenta z VPN można korzystać praktycznie z dowolnego systemu operacyjnego jak Windows, Mac, Linux, oraz różnych urządzeń mobilnych włączając w to iPhone, Windows Mobile, Symbian i Android.

Szczegółowe dane techniczne dotyczące wdrożonego urządzenia można znaleźć pod adresem: <http://www.juniper.net/us/en/products-services/security/sa-series/sa4500/>

Informacje wstępne.

Do skorzystania z usługi VPN niezbędny jest komputer osobisty z zainstalowanym systemem operacyjnym z rodziny Windows, Linux lub Mac OS, posiadający w zależności od systemu operacyjnego jedną z przeglądarek internetowych np. Internet Explorer, Mozilla FireFox, Opera, Safari, Chrome. Aby skorzystać z VPN komputer musi mieć połączenie z siecią Internet. Nie ma znaczenia, czy połączenie do sieci Internet jest realizowane poprzez usługę DSL, sieć komórkową, sieć TV kablowej, czy też w inny sposób. Nie ma również znaczenia, czy komputer jest bezpośrednio podłączony do sieci Internet, czy też za pośrednictwem routera (modemu TV kablowej, routera DSL itp). Na komputerze z którego łączymy się z usługą VPN musi być zainstalowane oprogramowanie antywirusowe z aktualną bazą. Tak samo system operacyjny, jak i pozostałe oprogramowanie musi być legalne. W przeciwnym razie narazamy się, że nasze dane dotyczące logowania do systemu VPN zostaną przechwycone przez osoby nieupoważnione.

Przy korzystaniu z usługi VPN należy wystrzegać się korzystania z komputerów np. w kafejkach internetowych i miejscach publicznych, co do których można mieć wątpliwości, czy na w/w sprzęcie nie ma zainstalowanego oprogramowania, które przechwytyje sekwencje naciskanych klawiszy lub rejestruje wymianę danych pomiędzy komputerem a siecią.

Zgodnie z przyjętymi zasadami nie wolno udostępniać danych do logowania, nazwy użytkownika i hasła innej osobie. Login i hasło są przeznaczone tylko i wyłącznie dla właściciela konta VPN i nikogo innego.

Pierwsze logowanie

Podczas pierwszego logowania do usługi VPN należy wykonać kilka prostych czynności konfiguracyjnych, które nie będą już konieczne przy kolejnych połączeniach. Czynności konfiguracyjne będą wymagały powtórzenia w przypadku re-instalacji systemu operacyjnego i/lub przeglądarki internetowej lub w przypadku połączenia z usługą VPN z innego komputera, z którego tego typu połączenia nie były wcześniej realizowane.

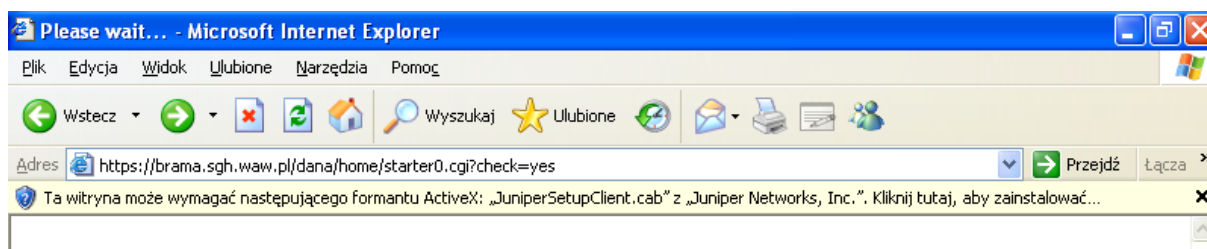


Rysunek 1 - Okno logowania

Chcąc połączyć się z usługą VPN należy uruchomić przeglądarkę internetową, a następnie w okienku adresu wpisać: <https://brama.sgh.waw.pl>. Jeśli połączenie z serwerem VPN zostanie zakończone powodzeniem w oknie przeglądarki pojawi się panel do logowania, analogiczny jak do przedstawionego rysunku (Rysunek 1 - Okno logowania).

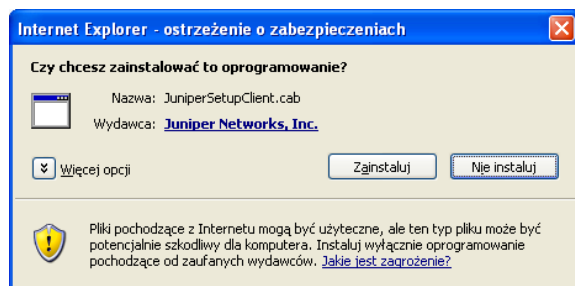
Następnie w polu "Login:" należy podać swoją nazwę użytkownika, identyczną jak używaną do logowania do domeny **SGH_NET**. W polu "Hasło" należy podać używane do logowania do domeny hasło.

Ostatnią czynnością do wykonania przed zalogowaniem się jest wybór działu, w którym dany użytkownik ma zdefiniowane uprawnienia. Wszyscy użytkownicy systemu VPN są domyślnie przypisani do działu o nazwie "domena Biblioteka".



Rysunek 2 - Komunikat o konieczności zainstalowania dodatku

Jeśli logowanie przebiegło prawidłowo w oknie przeglądarki na górze strony pojawi się komunikat o konieczności zainstalowania dodatku "JuniperSetupClient.cab" (Rysunek 2 - Komunikat o konieczności zainstalowania dodatku). Chcąc w pełni korzystać z funkcjonalności systemu VPN dodatek należy zainstalować klikając w link "Kliknij tutaj, aby zainstalować".



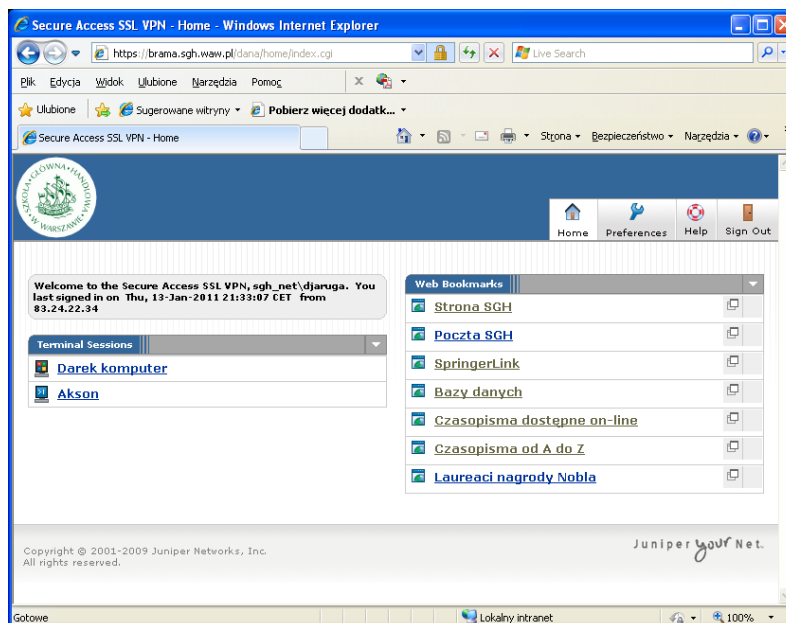
Rysunek 3 - Zgoda na instalację dodatku

W niektórych przypadkach, w zależności od aktualnych ustawień przeglądarki może pojawić się komunikat jak na rysunku (Rysunek 3 - Zgoda na instalację dodatku). Jeśli wystąpi należy potwierdzić zgodę na instalację dodatku.

Po zainstalowaniu dodatku system jest gotowy do pracy. W oknie przeglądarki pojawi się widok analogiczny do przedstawionego na rysunku (Rysunek 4 - Panel po zalogowaniu).

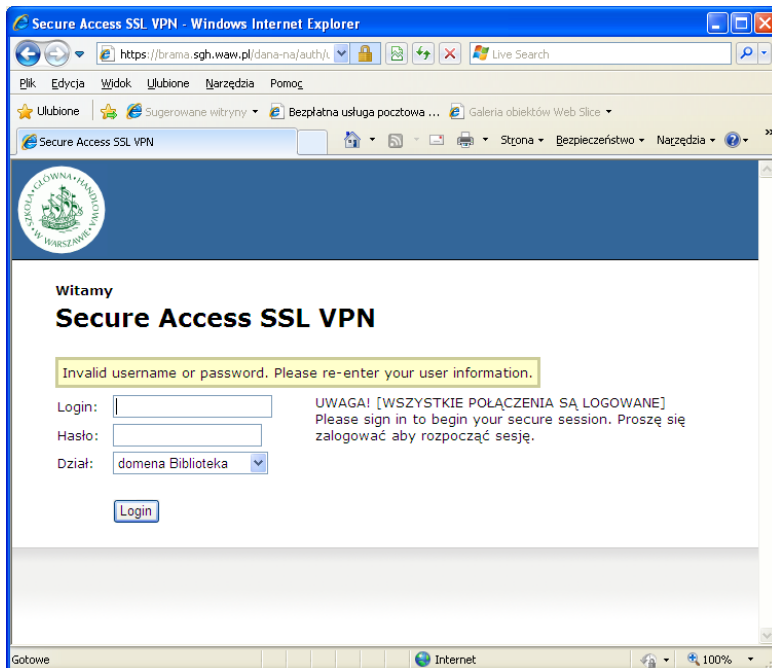
Od tej chwili jesteśmy zalogowani do usługi VPN i w pełni możliwe jest korzystanie z zasobów, których linki są dostępne w panelu "Home".

System VPN zapewnia dostęp do wskazanych wewnętrznych stron internetowych, dostęp do zdalnego pulpitu komputera osobistego do pracy w środowisku graficznym, dostęp do sesji terminalowej umożliwiającej pracę zdalną w trybie tekstowym. Ponadto możliwy jest dostęp do wewnętrznych zasobów dyskowych wskazanych przez administratora.



Rysunek 4 - Panel po zalogowaniu

W przypadku gdy logowanie do systemu VPN zostało zakończone porażką na skutek błędnie

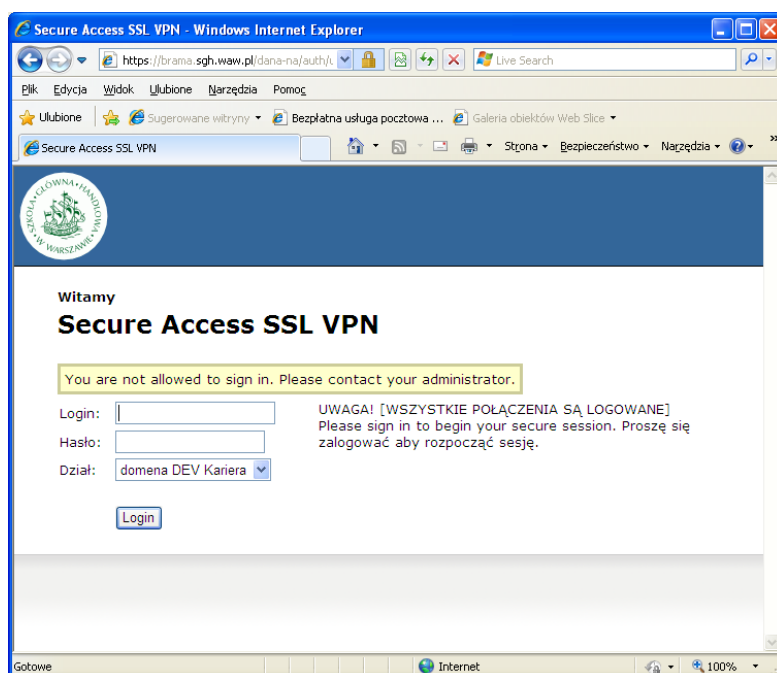


podanego loginu lub hasła w ekranie przeglądarki pojawi się komunikat "Invalid username or password. Please re-enter your user information" (Rysunek 5 - komunikat o błędnym loginie lub hasle.). Oznacza to, że podczas wpisywania nastąpił błąd i należy jeszcze raz podać nazwę użytkownika i hasło. Podając powtórnie hasło należy upewnić się, że nie jest wciśnięty klawisz CAPS LOCK.

Rysunek 5 - komunikat o błędnym loginie lub hasle.

Innym, częstym komunikatem błędu, z którym użytkownik może się spotkać jest brak uprawnień do danego działu.

Jeśli w panelu logowania poprawnie zostanie podana nazwa użytkownika i hasło, a błędnie wybrany dział w ekranie przeglądarki zostanie umieszczony komunikat: "You are not allowed to sign in. Please contact your administrator" (Rysunek 6 - brak uprawnień do działu). W takim przypadku w panelu logowania należy powtórnie wpisać login i hasło, a następnie wybrać właściwy dział. Wszyscy użytkownicy systemu VPN są domyślnie przypisani do działu o nazwie: "domena Biblioteka".



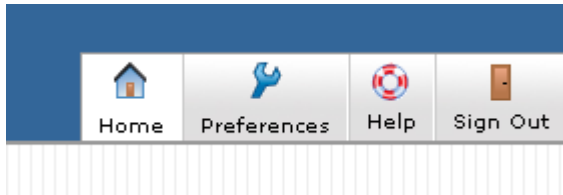
Rysunek 6 - brak uprawnień do działu

Kolejne logowania.

Wykonując kolejne logowanie do systemu VPN z tego samego komputera i tej samej przeglądarki w której został zainstalowany dodatek "JuniperSetupClient.cab" nie zachodzi konieczność powtórnego wykonywania instalacji w/w dodatku. Po podaniu loginu i hasła w oknie logowania i wybraniu właściwego działu w przeglądarce internetowej pojawi się panel z linkami do udostępnianych zasobów. Należy mieć jednak na względzie, że w przypadku opracowania przez producenta systemu VPN kolejnej nowszej wersji oprogramowania konieczność instalacji dodatku w nowej wersji pojawi się. W takim przypadku należy powtórzyć czynności jak dla pierwszego logowania.

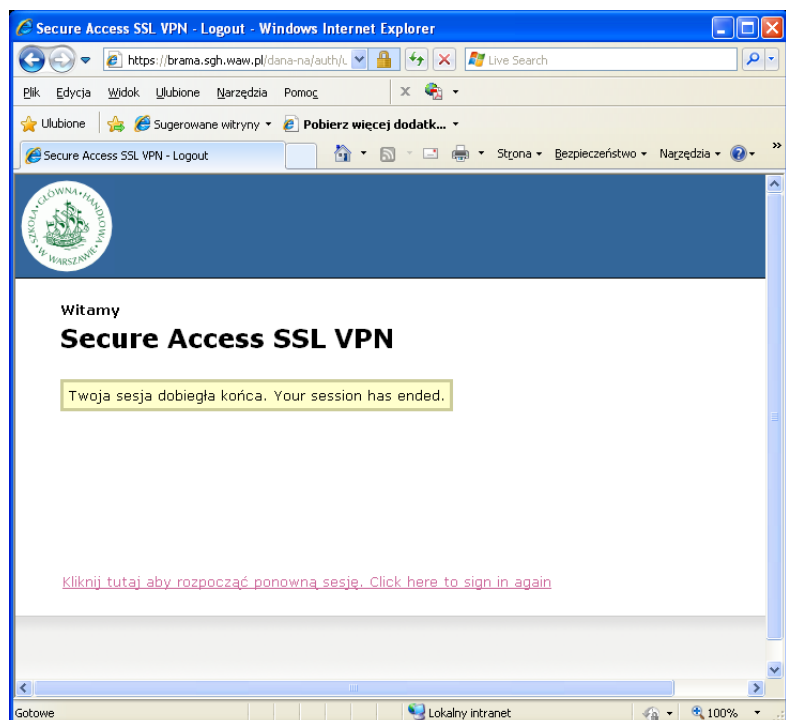
Zakończenie pracy z VPN.

System VPN został skonfigurowany w ten sposób, że w przypadku braku aktywności ze strony użytkownika sam rozłącza sesję i zamyka połączenie. Jednakże obowiązkiem każdego użytkownika jest zamykanie połączenia VPN w chwili gdy kończy pracę. W panelu systemu VPN znajduje się specjalny do tego przycisk o nazwie "Sign Out" (Rysunek 8 - przyciski nawigacyjne).

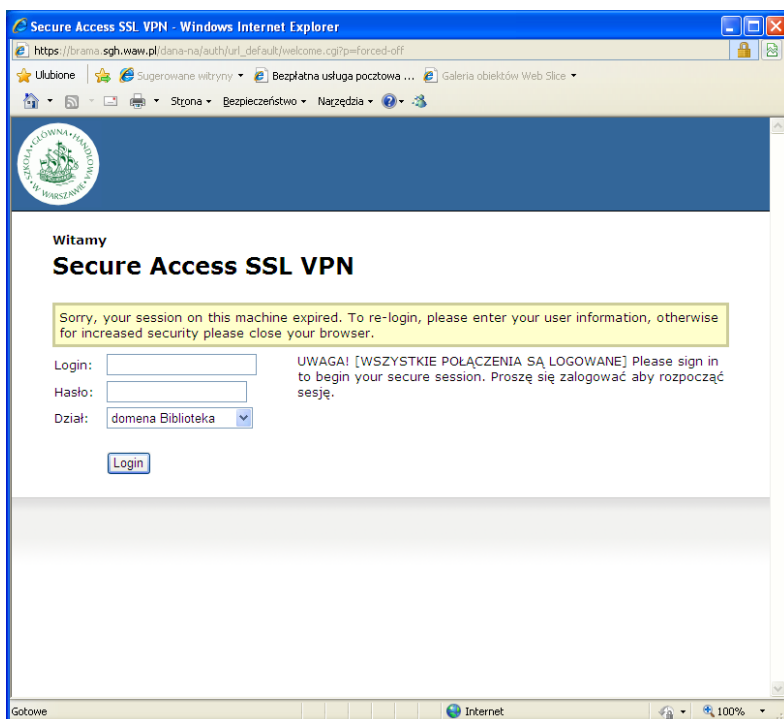


Rysunek 7 - przyciski nawigacyjne

Po prawidłowym wylogowaniu się z systemu VPN w oknie przeglądarki pojawi się komunikat: "Your session has ended." (Rysunek 8 - zakończenie sesji). W dolnej części okna przeglądarki znajduje się link, który pozwala na ponowne zalogowanie się do systemu VPN.



Rysunek 8 - zakończenie sesji



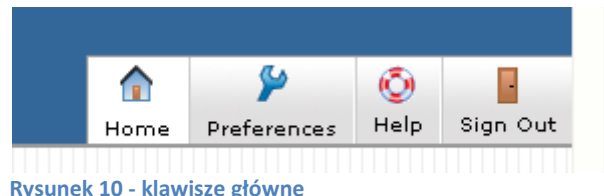
Rysunek 9 - wygaśnięcie sesji

W przypadku braku aktywności ze strony użytkownika po pewnym czasie system sam zamyka połączenie VPN. W takiej sytuacji w oknie przeglądarki pojawia się komunikat o treści: "Sorry, your session on this machine expired. To re-login, please enter your user information, otherwise for increased security please close your browser" (Rysunek 9 - wygaśnięcie sesji). Zgodnie z tym komunikatem, o ile nie zamierzamy dalej pracować z systemem VPN powinniśmy zamknąć okno przeglądarki lub jeszcze raz zalogować się jeśli zamierzamy pracę z VPN kontynuować.

Główne okno aplikacji VPN.

W głównym oknie systemu VPN zaraz po zalogowaniu się do dyspozycji użytkownika są cztery klawisze: "Home", "Preferences", "Help", "Sign Out" (Rysunek 10 - klawisze główne).

W kolejności klawisz "Home" otwiera okno z udostępnionymi zasobami, jest to domyślny widok, jaki użytkownik ma w oknie przeglądarki zaraz po zalogowaniu się.



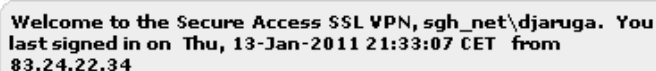
Rysunek 10 - klawisze główne

Klawisz "Preferences" umożliwia użytkownikowi skonfigurowanie wybranych elementów interfejsu systemu VPN np. kolejności wyświetlania informacji na stronie "Home".

Klawisz "Help" zawiera szczegółowy podręcznik użytkownika z zakresu obsługi systemu VPN.

Ostatni klawisz "Sign Out" służy do zakończenia pracy z systemem VPN i powinien być obowiązkowo wybierany w chwili zakończenia pracy z systemem.

Na stronie "Home" zaraz po zalogowaniu się, należy zwrócić uwagę na informację dotyczącą czasu i adresu IP ostatniego logowania (Rysunek 11 - informacja o ostatnim logowaniu). Jeśli podana tam informacja jest niezgodna z ostatnim logowaniem i jesteśmy pewni, że w danym czasie nie korzystaliśmy z połączeń VPN należy niezwłocznie zmienić hasło w udostępnionej pod adresem

The image shows a white rectangular box with a thin border. Inside, the text reads: "Welcome to the Secure Access SSL VPN, sgh_net\djaruga. You last signed in on Thu, 13-Jan-2011 21:33:07 CET from 83.24.22.34".

83.24.22.34

Rysunek 11 - informacja o ostatnim logowaniu

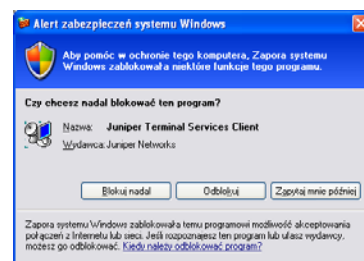
<https://akson.sgh.waw.pl/passwd/>

aplikacji i zgłosić ten fakt do Zespołu Pomocy Użytkownikom lub do administratora.

Klikając na poszczególne linki w udostępnionych zasobach wyświetlana jest strona WWW lub uruchamiana odpowiednia aplikacja zapewniająca zdalny dostęp np. usługa zdalnego pulpitu.

Osoby, które w swojej pracy z VPN będą korzystały z tekstowych połączeń terminalowych muszą na swoim komputerze zainstalować obsługę języka JAVA. Pakiet instalacyjny znajduje się do pobrania na stronie WWW pod adresem: <http://java.sun.com/>

Analogicznie w przypadku konieczności pracy ze zdalnym pulpitem w trybie graficznym zachodzi konieczność instalacji programu Juniper Terminal Services Client oraz odblokowanie dostępu do Internetu dla tej aplikacji w komputerze w aplikacji FireWall zainstalowanej na danej maszynie (Rysunek 12 - odblokowanie terminala VNC). W przypadku standardowego systemu FireWall wbudowanego w system Windows XP odblokowanie nastąpi po zatwierdzeniu wyjątku w okienku, które pojawi się na ekranie komputera podczas pierwszego uruchomienia.



Rysunek 12 - odblokowanie terminala VNC

Zakończenie

W niniejszej instrukcji przedstawiono podstawowe informacje dotyczące usługi VPN i sposobu korzystania. Osoby pragnące poszerzyć swoją wiedzę w zakresie VPN odsyłam do zamieszczonej w systemie VPN instrukcji użytkownika. Dla osób, dla których niniejsza instrukcja jest niewystarczająca, a podręcznik producenta zbyt skomplikowany zapraszam na szkolenie, które odbędzie się w dwóch terminach:

25 stycznia 2011 o godzinie 9:50 w sali 4A w budynku C,

26 stycznia 2011 o godzinie 9:50 w sali 2A w budynku C.