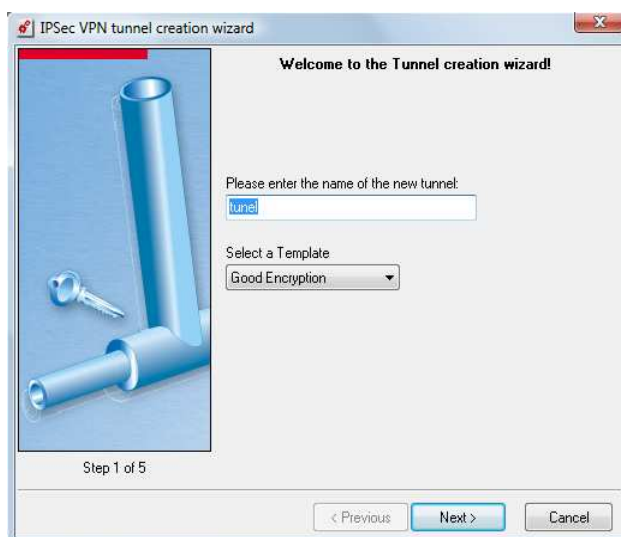


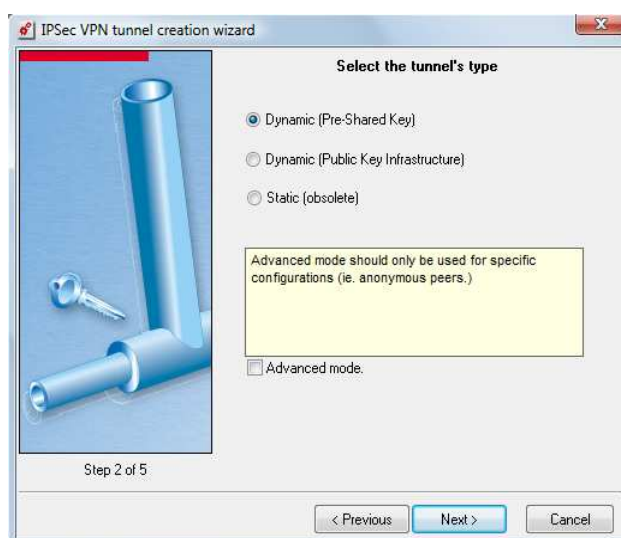
## Tworzenie bezpiecznego połączenia klient-to-site przy użyciu tunelu IPsec VPN

Do utworzenia bezpiecznego połączenia VPN potrzebna będzie uruchomiona aplikacja NETASQ Unified Manager, która wchodzi w skład dostarczanego przez producenta pakietu Administration Suite. Użytkownicy mobilni chcący się połączyć poprzez tunel VPN z siecią firmową muszą mieć zainstalowanego na swoich stacjach klienta IPsec VPN. Poniżej instrukcja jak stworzyć tunel IPsec VPN.

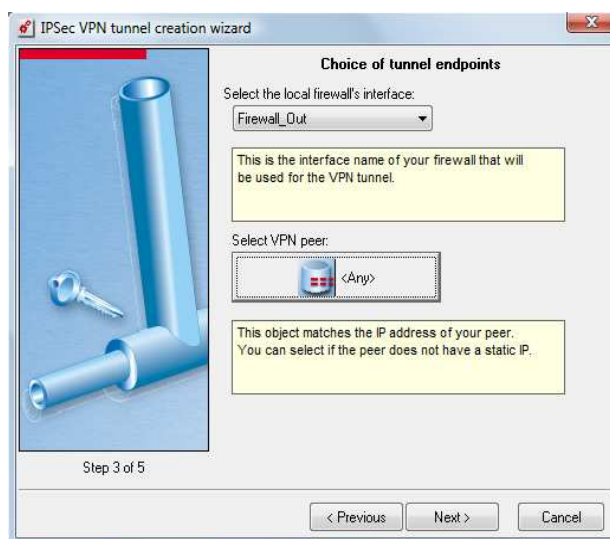
W lewym menu Unified Managera wejdź do sekcję **VPN → IPsecTunnels**. W nowym oknie wybierz z listy dowolny slot, czyli zestaw reguł i kliknij **Edit**, aby przejść do jego edytowania. Po uruchomieniu kreatora nadaj slotowi nazwę, która równocześnie będzie nazwą nowego tunelu. Szczegółowe ustawienia fazy tworzenia tunelu nie jest na tym etapie konieczne, dlatego możesz pozostawić ustawienia domyślne. Przejdź dalej klikając **Next**.



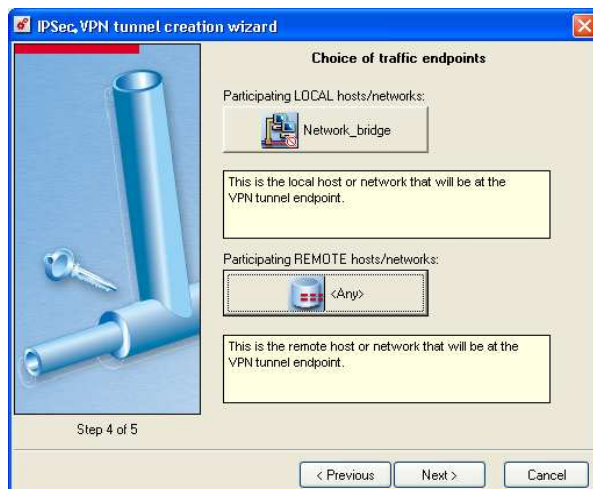
W następnym etapie wybierz typ autoryzacji. W przykładzie będzie to wymiana klucza współdzielonego. Zaznacz **Dynamic (Pre-Shared Key)** i kliknij **Next**.



Teraz wskaż adresy, które będą się ze sobą łączyć tworząc w ten sposób tunel VPN (**Tunnel Endpoints**).

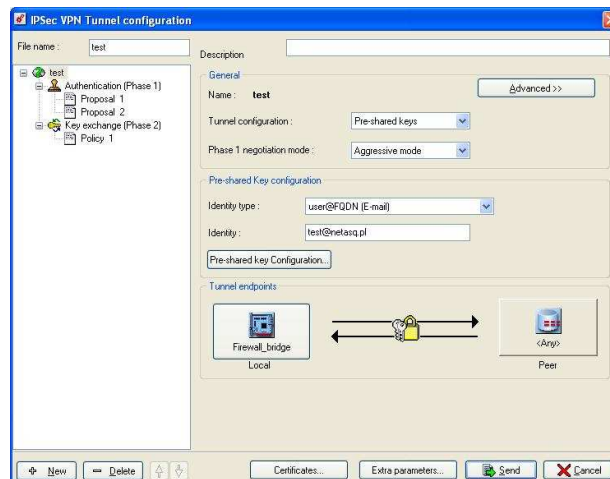


W opisywanym przykładzie chcemy połączyć użytkownika mobilnego z siedzibą firmy, dlatego użytkownik będzie się łączył z zewnętrznym interfejsem NETASQ. W polu „**Select local firewall's interface**” wskaż interfejs zewnętrzny urządzenia NETASQ (tutaj to interfejs **firewall\_out**). W sekcji „**Select VPN peer**” wytypuj drugi koniec tunelu, czyli adres z jakiego będzie łączył się użytkownik mobilny. Aby użytkownik mógł mieć dostęp do firmowej sieci lokalnej z dowolnego miejsca na świecie, obiekt jaki powinieneś wybrać w nowym oknie to **<Any>**. Zatwierdź **OK** i przejdź do kolejnego kroku konfiguracji klikając **Next**.

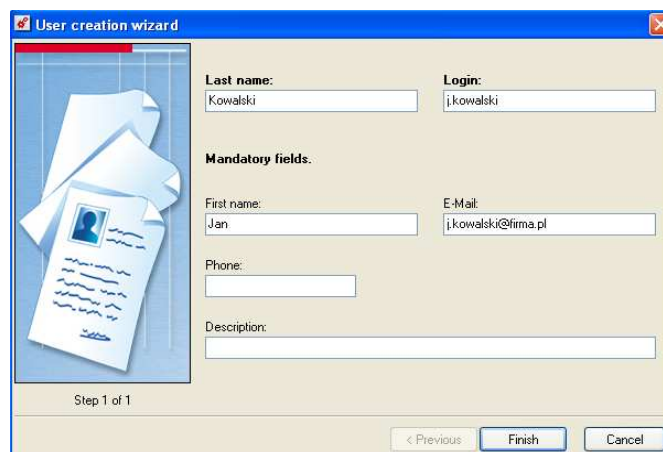


Następnie skonfiguruj **traffic endpoints**, czyli elementy dostępne dla obu końców tunelu VPN. W tym celu w sekcji **Local** wskaż elementy sieci po stronie firewalla (tutaj **Network\_brigde**), natomiast w sekcji **Remote** określ element dostępny po stronie zdalnej. W przypadku klienta mobilnego łączącego się z siecią lokalną, zdaną sieć wskaż jako obiekt **<Any>**.

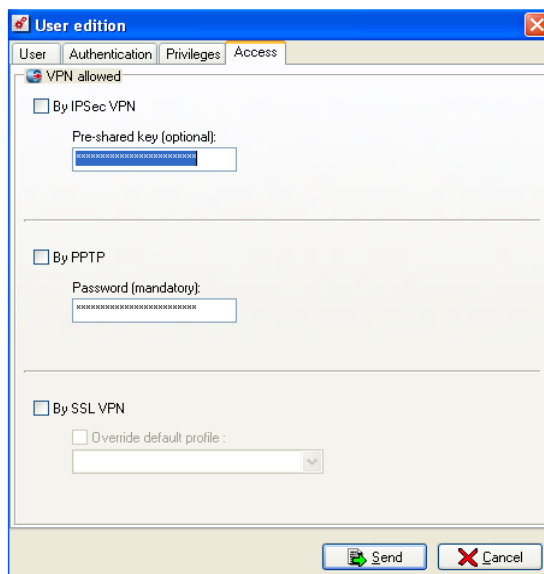
Po zakończeniu obsługi kreatora otwiera się okno z pełną konfiguracją VPN w edytowanym słocie. W tym przypadku skonfiguruj **pre-shared key**. W sekcji **General**, w fazie 1 (Phase 1 negotiation mode) wybierz **Agressive mode**, w **Identity type** wybierz **Email** i w polu **Identity** wprowadź adres email, jakim przedstawi się urządzenie NETASQ. Kliknij **Send**, potwierdź, a następnie zamknij okno z listą slotów.



W lewym menu głównego okna programu NETASQ Unified Manager wybierz sekcję **Objects** i stwórz nowego użytkownika **NEW**  **user**. Podaj jego imię, nazwisko, login oraz adres e-mail. Kliknij **Finish**.



W oknie edycji ustawień użytkownika przejdź do zakładki **Access**, zaznacz połączenie **by IPsec VPN**. Następnie w polu **Pre-shared key** wprowadź hasło, które zostanie udostępnione użytkownikowi. Za pomocą tego hasła odbywać będzie się autoryzacja. Wprowadzone ustawienia potwierdź przyciskiem **Send**. Zamknij okno ustawień naciskając **OK**.



Ponownie przejdź do sekcji **VPN → IPsec Tunnels**. Zaznacz nowo utworzony wcześniej slot o nazwie „tunel” i aktywuj jego działanie klikając **Activate** i zamknij okno.

W ostatnim etapie przejdź do sekcji **Policy → Filtering**. Edytuj dowolny slot i stwórz reguły zezwalające na połączenia przy wykorzystaniu IPsec VPN według prezentowanego schematu.

Status	Interface	DSCP	Service	Protocol	Message	Source	Source Port	Destination	Destination Port	Action	Routing	QoS	Log	ASQ options	Rule name	Description
1 On	auto			udp		<Any>	<Any>	Firewall_Out	isakmp	pass						
2 On	auto			udp		<Any>	<Any>	Firewall_Out	isakmp_natt	pass						
3 On	auto			vpn-esp		<Any>	<Any>	<Any>	<Any>	pass						
4 On	IPSec			all		<Any>	<Any>	<Any>	<Any>	pass						

Wyślij zmiany klikając **Send** oraz uruchom działanie slotu klikając **Activate**.

Aby zakończyć tworzenie tunelu należy pamiętać o zainstalowaniu i konfiguracji klienta IPsec VPN na stacji roboczej mobilnego użytkownika.