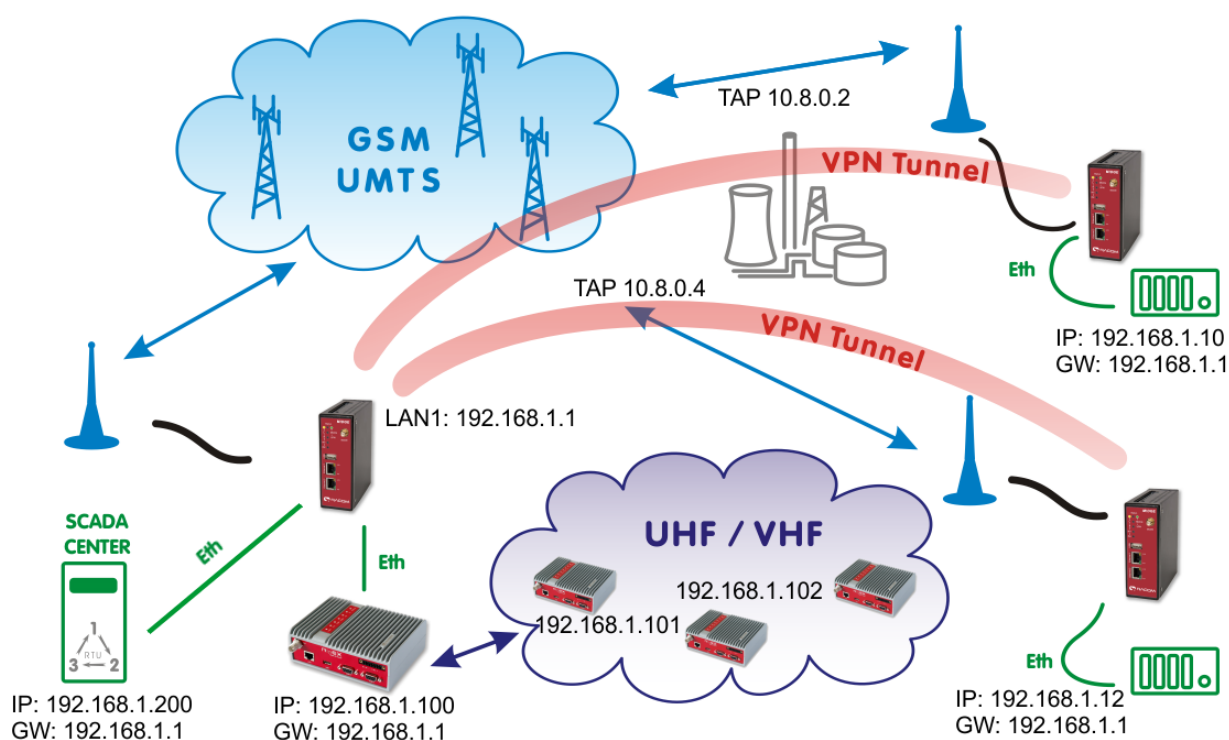


M!DGE

Koncentrator VPN



OpenVPN w trybie mostkowania (TAP)

Praca w warstwie drugiej modelu ISO/OSI

Dotyczy wersji oprogramowania 3.7
Wersja dokumentu: 1.0

Opracowanie:

KARCZ Polska
ul. Wilczak 16A, 61-626 Poznań
www.karcz.eu

Zawartość

WSTĘP.....	3
KROK 1 – WŁĄCZ SERWER OPENVPN	4
KROK 2 – KONFIGURACJA SERWERA	5
KROK 3 – WŁĄCZANIE KLIENTÓW.....	7
KROK 4 – KONFIGURACJA ZDALNYCH PODSIECI.....	8
KROK 5 – DODATKOWE PODSIECI W TUNELU OPENVPN	9
KROK 6 – GENEROWANIE PLIKÓW KONFIGURACYJNYCH	10
KROK 7 - KONFIGURACJA KLIENTÓW OPENVPN	12
KOMENTARZ.....	13
DIAGNOSTYKA	14
KONFIGURACJA KLIENTA TAP/TUN DLA WINDOWS	16
Lista zmian:	17

WSTĘP

Oprogramowanie OpenVPN służy do tworzenia wirtualnych sieci prywatnych (VPN) w **drugiej** lub **trzeciej** warstwie modelu [ISO/OSI](#). W zależności od konfiguracji tunel może przenosić pomiędzy podsieciami **ramki Ethernet** ([warstwa 2](#)) lub **pakiety IP** ([warstwa 3](#)). Za komunikację **Ethernet** odpowiada wirtualny interfejs [TAP](#). Tryb taki nazywa się mostkowaniem (bridging), ponieważ pozwala połączyć podsieci bez względu na używane w nich protokoły warstwy sieciowej.



Działanie tunelu w trybie **TAP** można porównać do 'switcha', gdzie każda pojawiająca się ramka jest powielana i przesyłana do wszystkich węzłów. Wadą rozwiązania jest **zwiększone zużycie pasma**, a zaletą **kompatybilność** z infrastrukturami bazującymi na starszych protokołach sieciowych.

Router MiDGE jest koncentrator OpenVPN, który pozwala na obsługę do 25¹ połączeń VPN.

Niniejszy dokument opisuje konfigurację **OpenVPN w trybie mostkowania**, krok po kroku.

UWAGA!

Przed przystąpieniem do pracy przygotuj urządzenia zgodnie z instrukcją [MiDGE – Pierwsze uruchomienie](#).

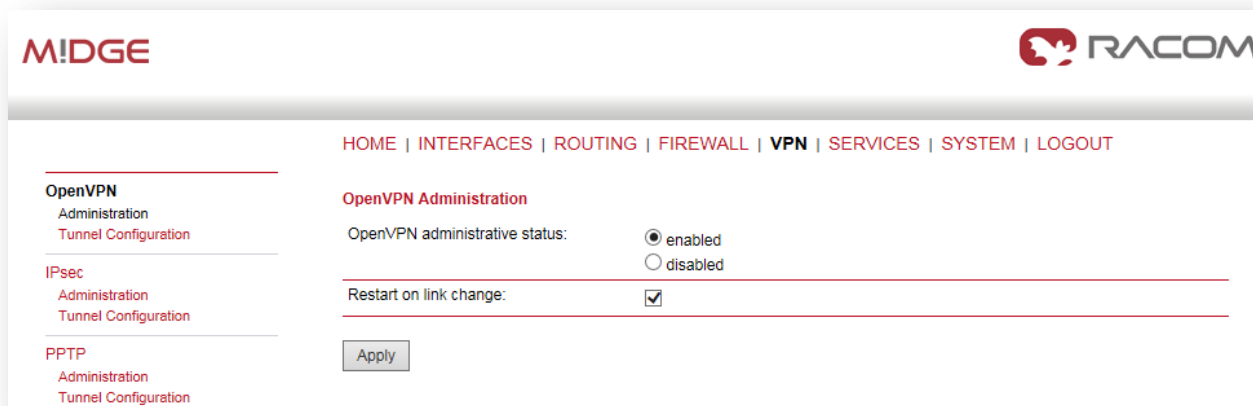
Aby utworzyć sieć prywatną VPN w technologii OpenVPN potrzebujesz jednego **stałego adresu IP** (karta SIM ze stałym adresem IP lub łącze DSL) lub usługi [DynamicDNS](#) (łącze ADSL – zmienne IP zewnętrzne) dla serwera. Urządzenia klienckie muszą mieć zapewniony podstawowy dostęp do Internetu bez ograniczeń dla ruchu wychodzącego.

Podłącz router do komputera poprzez port **ETH2** i wpisz w przeglądarkę adres <http://192.168.2.1>. Wykonując kolejne kroki zgodnie z instrukcją, port ETH1 zostanie przypisany do interfejsu TAP.

¹ Wymagane dodatkowe rozszerzenie funkcjonalne. Router standardowo obsługuje 10 połączeń VPN.

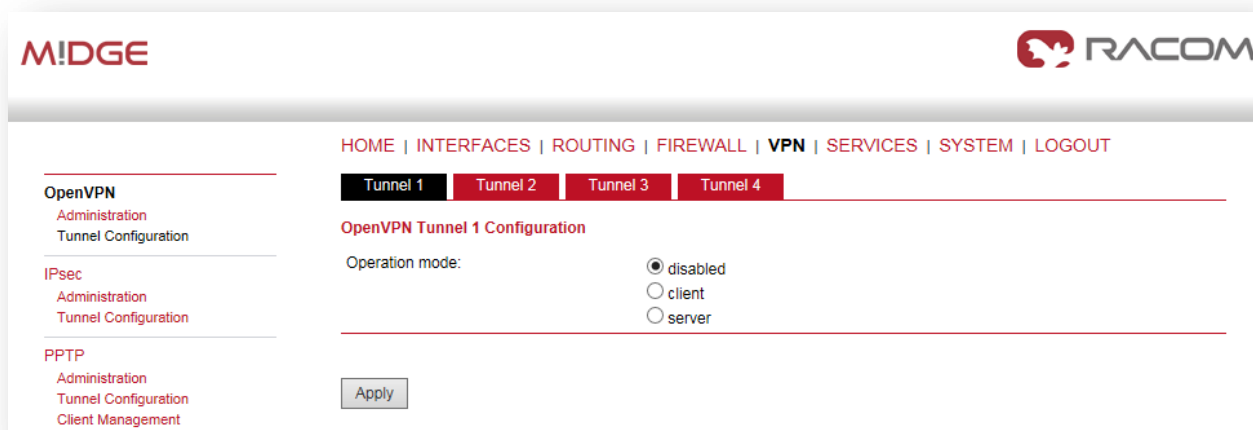
KROK 1 – WŁĄCZ SERWER OPENVPN

Po zalogowaniu do urządzenia przejdź do zakładki **VPN** i włącz usługę **OpenVPN**. Zaznacz 'enabled' i zatwierdź przyciskiem **Apply**



The screenshot shows the M!DGE web interface. The top navigation bar includes links: HOME | INTERFACES | ROUTING | FIREWALL | **VPN** | SERVICES | SYSTEM | LOGOUT. The left sidebar has a menu for OpenVPN with sub-items: Administration and Tunnel Configuration. The main content area is titled 'OpenVPN Administration'. It contains two settings: 'OpenVPN administrative status:' with radio buttons for 'enabled' (selected) and 'disabled', and 'Restart on link change:' with a checked checkbox. An 'Apply' button is at the bottom.

Następnie przejdź do opcji **Tunnel Configuration** i zaznacz opcję **Server**



The screenshot shows the 'OpenVPN Tunnel 1 Configuration' page. The top navigation bar is the same as the previous screenshot. The left sidebar has a menu for OpenVPN with sub-items: Administration, Tunnel Configuration, and Client Management. The main content area has tabs for Tunnel 1, Tunnel 2, Tunnel 3, and Tunnel 4. The 'OpenVPN Tunnel 1 Configuration' section contains the 'Operation mode:' setting with radio buttons for 'disabled' (selected), 'client', and 'server'. An 'Apply' button is at the bottom.

KROK 2 – KONFIGURACJA SERWERA

Po zmianie opcji otworzy się ekran konfiguracji serwera OpenVPN. W sekcji **Server port** możesz zmienić numer portu na dowolny, pod warunkiem, że nie będzie kolidował z innymi usługami. Z listy **Type** wybierz **TAP**, następnie w polu **Network mode**: zaznacz **bridged**. Pojawi się dodatkowe pole wyboru interfejsu LAN, który będzie przypisany do mostka tunelu. Wybierz **LAN1**. W sekcji **Options** zaznacz 'use keepalive', aby serwer podtrzymywał połączenie w czasie bezczynności.

HOME | INTERFACES | ROUTING | FIREWALL | VPN | SERVICES | SYSTEM | LOGOUT

Tunnel 1 Tunnel 2 Tunnel 3 Tunnel 4

OpenVPN Tunnel 1 Configuration

Operation mode: ☐ disabled ☐ client ☒ standard ☐ expert

Server port: 1194

Type: TAP

Protocol: UDP

Network mode: ☐ routed ☒ bridged MTU: Interface: LAN1

Cipher: BF-CBC

Authentication: certificate-based

HMAC digest: SHA1

Options: ☒ use compression ☐ redirect gateway ☒ use keepalive

Apply

Zatwierdź konfigurację przyciskiem **Apply**.

Dial-in Server

Cipher: BF-CBC

Authentication: certificate-based

HMAC digest: SHA1

root certificate, server certificate and server key are missing
Manage keys and certificates

Options: ☒ use compression ☐ redirect gateway ☐ use keepalive

Apply Erase

Router zażąda wygenerowania certyfikatów niezbędnych do szyfrowania połączenia. Kliknij w link **Manage keys and certificates**. Komunikat nie pojawi się, jeżeli wcześniej zainstalowałeś własne certyfikaty.

Teraz wygeneruj certyfikaty serwera OpenVPN, klikając na przycisk **CREATE**.

HOME | INTERFACES | ROUTING | FIREWALL | VPN | SERVICES | **SYSTEM** | LOGOUT

Root CA | WebServer | SSH | **OpenVPN1** | Other

OpenVPN1

The keys/certificates used for authenticating the OpenVPN tunnel

Tunnel1 is running in server mode with certificates ([configure](#))

☒ generate keys/certificates
☐ upload pre-generated keys/certificates

Server certificate	missing
Private key	missing
CA root certificate	missing

[Create](#)

System wygeneruje certyfikaty niezbędne do autoryzacji i szyfrowania danych w tunelu VPN.

Processing...

The device is processing a key/certificate request, please stand by.

» Generating key for openvpn-tunnel0

Po zakończeniu pracy wróć do konfiguracji OpenVPN, klikając na link **configure**

HOME | INTERFACES | ROUTING | FIREWALL | VPN | SERVICES | **SYSTEM** | LOGOUT

Root CA | WebServer | SSH | **OpenVPN1** | Other

OpenVPN1

The keys/certificates used for authenticating the OpenVPN tunnel

Tunnel1 is running in server mode with certificates ([configure](#))

☒ generate keys/certificates
☐ upload pre-generated keys/certificates

Server certificate	view
Private key	view
CA root certificate	view

[Apply](#) [Delete](#)

Client Certificates for Tunnel1

Client1	Create
---------	------------------------

KROK 3 – WŁĄCZANIE KLIENTÓW

Teraz czas na przygotowanie użytkowników zdalnych, czyli Klientów OpenVPN. Przejdź do menu **Client Management** i klikając w pole zaznaczenia (checkbox) włącz żadaną liczbę klientów OpenVPN czyli wirtualnych portów ETH. Proponujemy każdemu użytkownikowi przypisać nazwę, która pozwoli na identyfikowanie połączeń lub obiektów.

HOME | INTERFACES | ROUTING | FIREWALL | **VPN** | SERVICES | SYSTEM | LOGOUT

Clients | **Networking** | Routes | Download

Client Management

Enabled	Client	Connection info
<input checked="" type="checkbox"/>	STACJA_1	
<input checked="" type="checkbox"/>	STACJA_2	
<input type="checkbox"/>	Client3	
<input type="checkbox"/>	Client4	
<input type="checkbox"/>	Client5	
<input type="checkbox"/>	Client6	
<input type="checkbox"/>	Client7	
<input type="checkbox"/>	Client8	
<input type="checkbox"/>	Client9	
<input type="checkbox"/>	Client10	

Apply Refresh

Zatwierdź operację przyciskiem **Apply**. Status klientów zmieni się na 'not connected'. Przejdź do zakładki **NETWORKING**.

HOME | INTERFACES | ROUTING | FIREWALL | **VPN** | SERVICES | SYSTEM | LOGOUT

Clients | **Networking** | Routes | Download

Client Management

Enabled	Client	Connection info
<input checked="" type="checkbox"/>	STACJA_1	not connected
<input checked="" type="checkbox"/>	STACJA_2	not connected
<input type="checkbox"/>	Client3	
<input type="checkbox"/>	Client4	
<input type="checkbox"/>	Client5	
<input type="checkbox"/>	Client6	
<input type="checkbox"/>	Client7	
<input type="checkbox"/>	Client8	
<input type="checkbox"/>	Client9	
<input type="checkbox"/>	Client10	

Uwaga!

Możesz wygenerować tylko jeden plik konfiguracyjny dla wszystkich 'klientów', ponieważ adresy w tunelu transportowym są przydzielane dynamicznie. Sugerujemy utworzenie 'listy klientów' OpenVPN, co ułatwi zarządzanie i diagnostykę sieci.

KROK 4 – KONFIGURACJA ZDALNYCH PODSIECI

W tym miejscu możesz zmienić adres IP podsieci transportowej, przypisać na stałe adresy tunelu dla poszczególnych klientów oraz ich podsieci. W trybie **TAP** nie jest wymagane definiowanie zdalnych podsieci, ponieważ usługa działa w trybie mostkowania. Ewentualne zmiany nie mają wpływu na pracę tunelu. Proponujemy pozostawić ustawienia domyślne i przejść do zakładki **DOWNLOAD**.

HOME | INTERFACES | ROUTING | FIREWALL | **VPN** | SERVICES | SYSTEM | LOGOUT

Clients | **Networking** | Routes | Download

OpenVPN
Administration
Tunnel Configuration
Client Management

IPsec
Administration
Tunnel Configuration

PPTP
Administration
Tunnel Configuration
Client Management

GRE
Administration
Tunnel Configuration

Dial-in Server

Transport Network

Network: 10.8.0.0

Netmask: 255.255.255.0

Client Networks

This menu can be used to configure a fixed tunnel endpoint address for each client. You may also specify a network whose packets should get routed towards the client.

Select client: STACJA_1

Tunnel address: ☒ dynamic ☐ fixed

Client network: ☒ none ☐ specify

Apply

Wskazówka

Można zastosować pewne udogodnienie dla celów testowych. Domyślna sieć transportowa to 10.8.0.0 i z tej puli adresowej serwer będzie przydzielał adresy dla interfejsów TAP. Wysyłanie pakietów 'ping' z podsieci 192.168.1.0/24 do podsieci tunelu 10.8.0.0/24 bez konfiguracji tablicy routingu nie jest możliwe. Jeżeli w tym miejscu podamy adres naszej podsieci, czyli 192.168.0.0/255.255.255.0, to każda wirtualna karta **TAP** otrzyma adres z tej samej puli, co sieć robocza. Zmniejsza to jednak pojemność podsieci i wprowadza konieczność planowania zasobów. Rozwiązanie umożliwia diagnostykę całej sieci, jednak nie jest to konieczne, ponieważ lista klientów oraz ich status pracy dostępne są w zakładce **VPN -> OpenVPN -> Client Management -> Clients** - patrz strona 15 – Diagnostyka.

KROK 5 – DODATKOWE PODSIECI W TUNELU OPENVPN

Po zakończeniu konfiguracji Klientów przejdź do zakładki **Routes**. Sieć w trybie mostkowania (bridged) nie korzysta z routingu, więc wszystkie pola pozostawiamy puste.

HOME | INTERFACES | ROUTING | FIREWALL | **VPN** | SERVICES | SYSTEM | LOGOUT

Clients | Networking | **Routes** | Download

Client Routes

This list of network routes will be pushed to each client, so that matching packets will be routed back to the server.

Network	Netmask
<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>

Enable routing between clients: ☐

Apply

KROK 6 – GENEROWANIE PLIKÓW KONFIGURACYJNYCH

W zakładce **DOWNLOAD** pole *Server address/hostname* system wypełnia numerem IP aktywnego łącza internetowego. Sprawdź czy numer IP się zgadza z przydzielonym od operatora. Jeżeli korzystasz z usługi **DynamicDNS** wprowadź w tym miejscu nazwę hosta. Następnie kliknij na przycisk **Download**. MiDGE wygeneruje pliki konfiguracyjne dla klientów OpenVPN.

The screenshot shows the MiDGE VPN configuration interface. The top navigation bar includes links: HOME | INTERFACES | ROUTING | FIREWALL | **VPN** | SERVICES | SYSTEM | LOGOUT. Below this, a sub-navigation bar has tabs: Clients | Networking | Routes | **Download**. The main content area is titled 'Download Expert Mode Files'. It contains a text input field for 'Server address/hostname' with the value '31.61.' and a 'Download' button. On the left side, there is a sidebar menu with categories: OpenVPN (Administration, Tunnel Configuration, Client Management), IPsec (Administration, Tunnel Configuration), PPTP (Administration, Tunnel Configuration, Client Management), GRE (Administration, Tunnel Configuration), and Dial-in Server.

Generowanie plików konfiguracyjnych dla klientów.

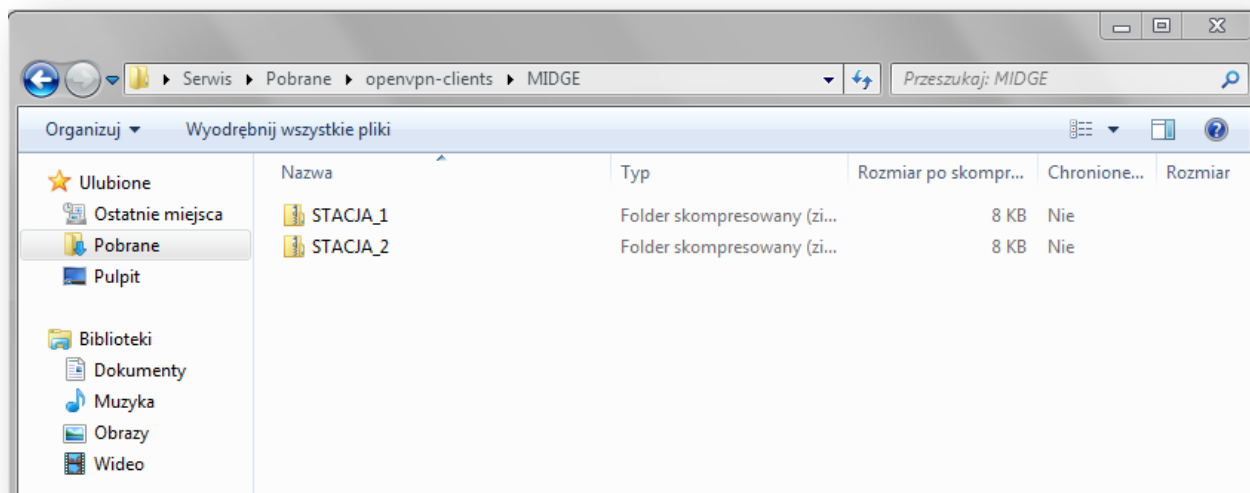
This screenshot shows the 'Processing...' status of the file generation. The top navigation bar is the same as the previous screenshot. The sub-navigation bar remains 'Clients | Networking | Routes | **Download**'. The main content area now displays 'Processing...' and a message: 'Generating expert mode files for all enabled OpenVPN clients, please stand by.' Below this, there are two status messages: '» Creating expert mode file for 'STACJA_1'' and '» Creating expert mode file for 'STACJA_2''. The sidebar menu on the left is identical to the previous screenshot.

Kiedy router zakończy pracę, zapisz archiwum **openvpn-clients.zip**

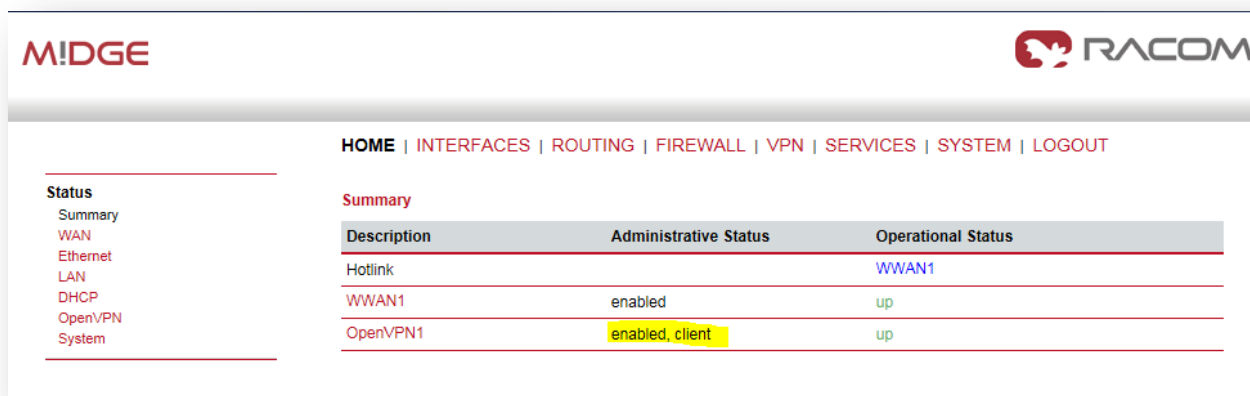
This screenshot shows the successful completion of the file generation process. The top navigation bar and sub-navigation bar are the same. The main content area now displays a green checkmark icon and the message: '2015-03-10 14:18 Successfully created expert mode files'. The 'Download' button is still present. At the bottom of the interface, a dialog box is open, asking: 'Czy chcesz otworzyć lub zapisać plik openvpn-clients.zip (16,0 KB) z witryny 192.168.10.1?'. The dialog has three buttons: 'Otwórz', 'Zapisz' (highlighted in yellow), and 'Anuluj', along with a close button (X).

Plik archiwum **openvpn-clients.zip** należy wypakować na dysk lub kluczu USB. Wewnątrz pliku znajdują się archiwa o nazwach zgodnych z utworzonymi klientami OpenVPN. Do konfiguracji klientów w urządzeniach MiDGE używamy plików skompresowanych, w tym przykładzie *STACJA_1.zip*, *STACJA_2.zip*.

Wygenerowany plik konfiguracyjny jest zgodny z pakietem OpenVPN. Możesz więc użyć go do konfiguracji innych urządzeń, które wspierają OpenVPN.



W zakładce **HOME** widoczny jest status pracy serwera. Na panelu urządzenia zaświeci się **zielona dioda**, sygnalizująca gotowość serwera do pracy.



**Na tym etapie zakończyłeś konfigurację serwera OpenVPN.
MiDGE jest gotowy do pracy jako koncentrator VPN.**

KROK 7 - KONFIGURACJA KLIENTÓW OPENVPN

Konfiguracja *Klientów OpenVPN* sprowadza się do włączenia usługi oraz wgrania pliku konfiguracyjnego oraz przydzielenia karty sieciowej dla interfejsu TAP.

Zaloguj się do urządzenia, przejdź do zakładki **VPN**, włącz usługę **OpenVPN** zaznaczając *enable* i zatwierdź przyciskiem **Apply**. Kiedy usługa zostanie uruchomiona (pojawi się przycisk **Restart** obok **Apply**). Dalej w menu **Tunnel Configuration** zaznacz wszystko zgodnie z rysunkiem. Wskaż plik konfiguracyjny i zatwierdź przyciskiem **Apply**.

HOME | INTERFACES | ROUTING | FIREWALL | **VPN** | SERVICES | SYSTEM | LOGOUT

Tunnel 1 Tunnel 2 Tunnel 3 Tunnel 4

OpenVPN Tunnel 1 Configuration

Operation mode: ☐ disabled ☒ **client** ☐ standard ☐ server ☒ **expert**

Network mode: ☐ routed ☒ **bridged** Interface: **LAN1**

Expert mode file (zip): **STACJA_1.zip**

Po wczytaniu pliku konfiguracyjnego system potwierdzi operację komentarzem - **installed**.

W zakładce **HOME** widoczny jest status pracy tunelu OpenVPN.

M!DGE RACOM

HOME | INTERFACES | ROUTING | FIREWALL | **VPN** | SERVICES | SYSTEM | LOGOUT

Status

Summary
WAN
Ethernet
LAN
DHCP
OpenVPN
System

Summary

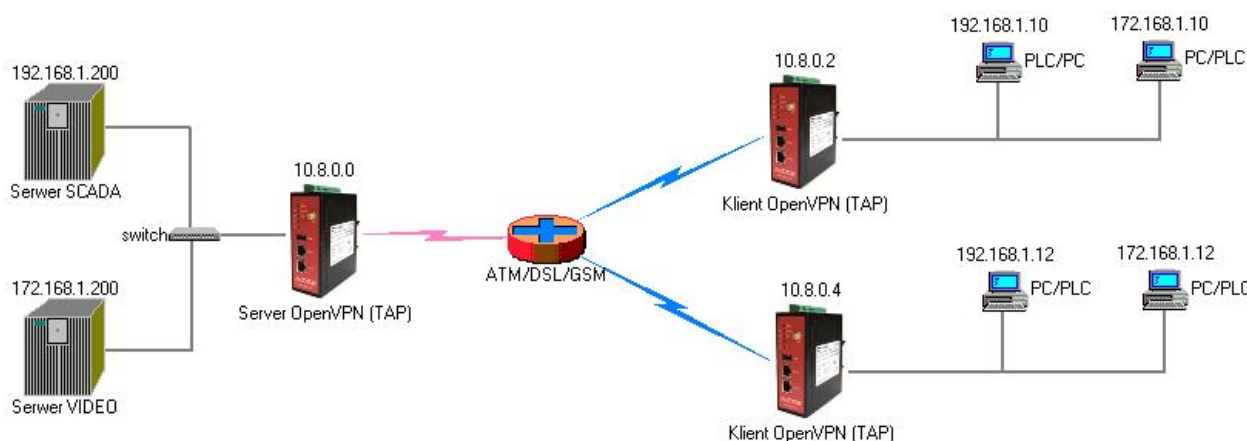
Description	Administrative Status	Operational Status
Hotlink		WWAN1
WWAN1	enabled	up
OpenVPN1	enabled, client	up

Konfigurację kolejnych urządzeń przeprowadź w analogiczny sposób, powtarzając **Krok 7**.

Teraz możesz podłączyć urządzenia do portu **LAN1** (można zastosować dodatkowy switch) i skonfigurować ich karty sieciowe, przydzielając adresy IP (możesz też skorzystać z serwera DHCP). Pamiętaj, że konfigurujesz „wirtualną sieć lokalną” więc bramą domyślną w sieci jest serwer OpenVPN - w tym przykładzie **192.168.1.1**, maska podsieci **255.255.255.0**

KOMENTARZ

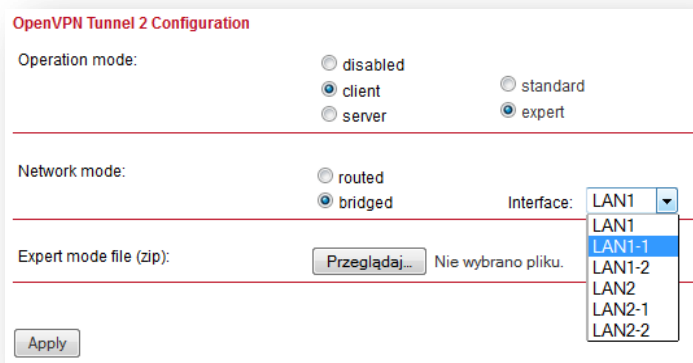
Usługa OpenVPN w trybie mostkowania (TAP) oferuje dużo większe możliwości niż tryb routera (TUN). Jest możliwa komunikacja po adresach MAC, stosowanie tablic ARP, etc. Należy jednak pamiętać o tym, że tryb TAP generuje większy ruch na łączach w związku z czym słabsze połączenia jak GPRS/UMTS mogą się „przytykać” - oczywiście zależy to również od ruchu generowanego w sieci roboczej. Zalecamy jednak zadbać o łącze o przepustowości min. 1Mbps. Technologia HSPA+ pozwala na uzyskanie połączenia o przepustowości do 5.76Mbps.



Rys. Przykładowa sieć wykorzystująca mostkowanie w tunelu OpenVPN.

Urządzenia MiDGE pozwalają na obsługę do 4 klientów VPN. W swojej sieci możesz więc użyć do 4 serwerów OpenVPN. Możliwe jest odseparowanie dwóch sieci od siebie, np. przemysłowej od sieci monitoringu wizyjnego. Do tunelu w trybie *bridged* (TAP) można przypisać również porty [VLAN](#), co pozwoli w pełni wykorzystać potencjał routera [MiDGE](#).

Konfiguracja **IP Settings** LAN1/LAN2 w urządzeniach klienckich nie ma znaczenia. Jeżeli chcesz aby port ETH1 był widoczny w sieci roboczej, np. w celu diagnostyki za pomocą pakietów ICMP, to możesz przypisać mu wolne IP z podsieci roboczej, np. 192.168.1.50.



Niniejszą instrukcję należy traktować jako podstawę dla własnych testów. Możesz użyć mocniejszego szyfrowania, zewnętrznych certyfikatów SSL, czy protokołu TCP zamiast UDP, zewnętrznego serwera DHCP, itd.

DIAGNOSTYKA

Status połączeń widoczny jest w zakładce **VPN->Client Management->Clients** po stronie serwera.

The screenshot shows the MIDGE Web Manager interface. The top navigation bar includes links to HOME, INTERFACES, ROUTING, FIREWALL, VPN, SERVICES, SYSTEM, and LOGOUT. The left sidebar contains navigation options for OpenVPN, IPsec, and PPTP. The main content area is titled 'Client Management' and displays a table of active clients. The table has three columns: 'Enabled', 'Client', and 'Connection info'. The clients listed are STACJA_1, STACJA_2, SCADA, and SERWIS. STACJA_1, STACJA_2, and SCADA are connected, while SERWIS is not connected.

Enabled	Client	Connection info
<input checked="" type="checkbox"/>	STACJA_1	from 95.50. [redacted] (10.8.0.3) since 2015-04-07 13:31:55
<input checked="" type="checkbox"/>	STACJA_2	from 31.61. [redacted] (10.8.0.5) since 2015-04-07 13:26:24
<input checked="" type="checkbox"/>	SCADA	from 95.50. [redacted] (10.8.0.2) since 2015-04-07 13:29:34
<input checked="" type="checkbox"/>	SERWIS	not connected

Podłącz komputer PC do serwera lub jednego z klientów i odpytaj poleceniem 'ping' pozostałe urządzenia. Możesz skorzystać również z polecenia ARP, np. arp -a. Poniżej diagnostyka testowej sieci.

```
C:\Users\Serwis>ping 192.168.1.1 (Serwer OpenVPN - sieć GSM)
```

Badanie 192.168.1.1 z 32 bajtami danych:

```
Odpowiedź z 192.168.1.1: bajtów=32 czas=73ms TTL=64
Odpowiedź z 192.168.1.1: bajtów=32 czas=75ms TTL=64
Odpowiedź z 192.168.1.1: bajtów=32 czas=71ms TTL=64
Odpowiedź z 192.168.1.1: bajtów=32 czas=78ms TTL=64
```

Statystyka badania ping dla 192.168.1.1:

```
Pakiety: Wysłane = 4, Odebrane = 4, Utracone = 0 (0% straty),
Szacunkowy czas błędzenia pakietów w milisekundach:
Minimum = 71 ms, Maksimum = 78 ms, Czas średni = 74 ms
```

```
C:\Users\Serwis>ping 192.168.1.10 (STACJA_1 - sieć PSTN/xDSL)
```

Badanie 192.168.1.10 z 32 bajtami danych:

```
Odpowiedź z 192.168.1.10: bajtów=32 czas=140ms TTL=128
Odpowiedź z 192.168.1.10: bajtów=32 czas=145ms TTL=128
Odpowiedź z 192.168.1.10: bajtów=32 czas=134ms TTL=128
Odpowiedź z 192.168.1.10: bajtów=32 czas=154ms TTL=128
```

Statystyka badania ping dla 192.168.1.10:

```
Pakiety: Wysłane = 4, Odebrane = 4, Utracone = 0 (0% straty),
Szacunkowy czas błędzenia pakietów w milisekundach:
Minimum = 134 ms, Maksimum = 154 ms, Czas średni = 143 ms
```

```
C:\Users\Serwis>ping 192.168.1.12 (STACJA_2 - sieć GSM)
```

Badanie 192.168.1.12 z 32 bajtami danych:

```
Odpowiedź z 192.168.1.12: bajtów=32 czas=487ms TTL=128
Odpowiedź z 192.168.1.12: bajtów=32 czas=170ms TTL=128
Odpowiedź z 192.168.1.12: bajtów=32 czas=155ms TTL=128
Odpowiedź z 192.168.1.12: bajtów=32 czas=166ms TTL=128
```

Statystyka badania ping dla 192.168.1.12:

```
Pakiety: Wysłane = 4, Odebrane = 4, Utracone = 0 (0% straty),
Szacunkowy czas błędzenia pakietów w milisekundach:
Minimum = 155 ms, Maksimum = 487 ms, Czas średni = 244 ms
```

```
C:\Users\Serwis>ping 192.168.1.101 (sieć radiowa - router RipEX)
Badanie 192.168.1.101 z 32 bajtami danych:
Odpowiedź z 192.168.1.101: bajtów=32 czas=907ms TTL=63
Odpowiedź z 192.168.1.101: bajtów=32 czas=138ms TTL=63
Odpowiedź z 192.168.1.101: bajtów=32 czas=120ms TTL=63
Odpowiedź z 192.168.1.101: bajtów=32 czas=137ms TTL=63
```

```
Statystyka badania ping dla 192.168.1.101:
    Pakiety: Wysłane = 4, Odebrane = 4, Utracone = 0 (0% straty),
Szacunkowy czas błędzenia pakietów w millisekundach:
    Minimum = 120 ms, Maksimum = 907 ms, Czas średni = 325 ms
```

```
C:\Users\Serwis>ping 192.168.1.102 (sieć radiowa - router RipEX)
Badanie 192.168.1.102 z 32 bajtami danych:
Odpowiedź z 192.168.1.102: bajtów=32 czas=948ms TTL=63
Odpowiedź z 192.168.1.102: bajtów=32 czas=141ms TTL=63
Odpowiedź z 192.168.1.102: bajtów=32 czas=135ms TTL=63
Odpowiedź z 192.168.1.102: bajtów=32 czas=151ms TTL=63
```

```
Statystyka badania ping dla 192.168.1.102:
    Pakiety: Wysłane = 4, Odebrane = 4, Utracone = 0 (0% straty),
Szacunkowy czas błędzenia pakietów w millisekundach:
    Minimum = 135 ms, Maksimum = 948 ms, Czas średni = 343 ms
```

```
C:\Users\Serwis>ping 192.168.1.200 (serwer SCADA - VLAN)
Badanie 192.168.1.200 z 32 bajtami danych:
Odpowiedź z 192.168.1.200: bajtów=32 czas<1 ms TTL=128
Odpowiedź z 192.168.1.200: bajtów=32 czas<1 ms TTL=128
Odpowiedź z 192.168.1.200: bajtów=32 czas<1 ms TTL=128
Odpowiedź z 192.168.1.200: bajtów=32 czas<1 ms TTL=128
```

```
Statystyka badania ping dla 192.168.1.200:
    Pakiety: Wysłane = 4, Odebrane = 4, Utracone = 0 (0% straty),
Szacunkowy czas błędzenia pakietów w millisekundach:
    Minimum = 0 ms, Maksimum = 0 ms, Czas średni = 0 ms
```

```
C:\Users\Serwis>arp -a
```

```
Interfejs: 192.168.1.200 --- 0x14
```

Adres internetowy	Adres fizyczny	Typ
10.8.0.0	00-ff-09-8c-c1-75	dynamiczne
192.168.1.1	00-02-a9-ff-ca-8b	dynamiczne
192.168.1.10	00-ff-f3-0e-68-48	dynamiczne
192.168.1.12	00-ff-86-17-4b-5c	dynamiczne
192.168.1.100	00-02-a9-a3-46-2a	dynamiczne
192.168.1.101	00-02-a9-a3-46-2a	dynamiczne
192.168.1.102	00-02-a9-a3-46-2a	dynamiczne
192.168.1.255	ff-ff-ff-ff-ff-ff	statyczne
224.0.0.2	01-00-5e-00-00-02	statyczne
224.0.0.22	01-00-5e-00-00-16	statyczne
224.0.0.252	01-00-5e-00-00-fc	statyczne
239.255.255.250	01-00-5e-7f-ff-fa	statyczne
255.255.255.255	ff-ff-ff-ff-ff-ff	statyczne

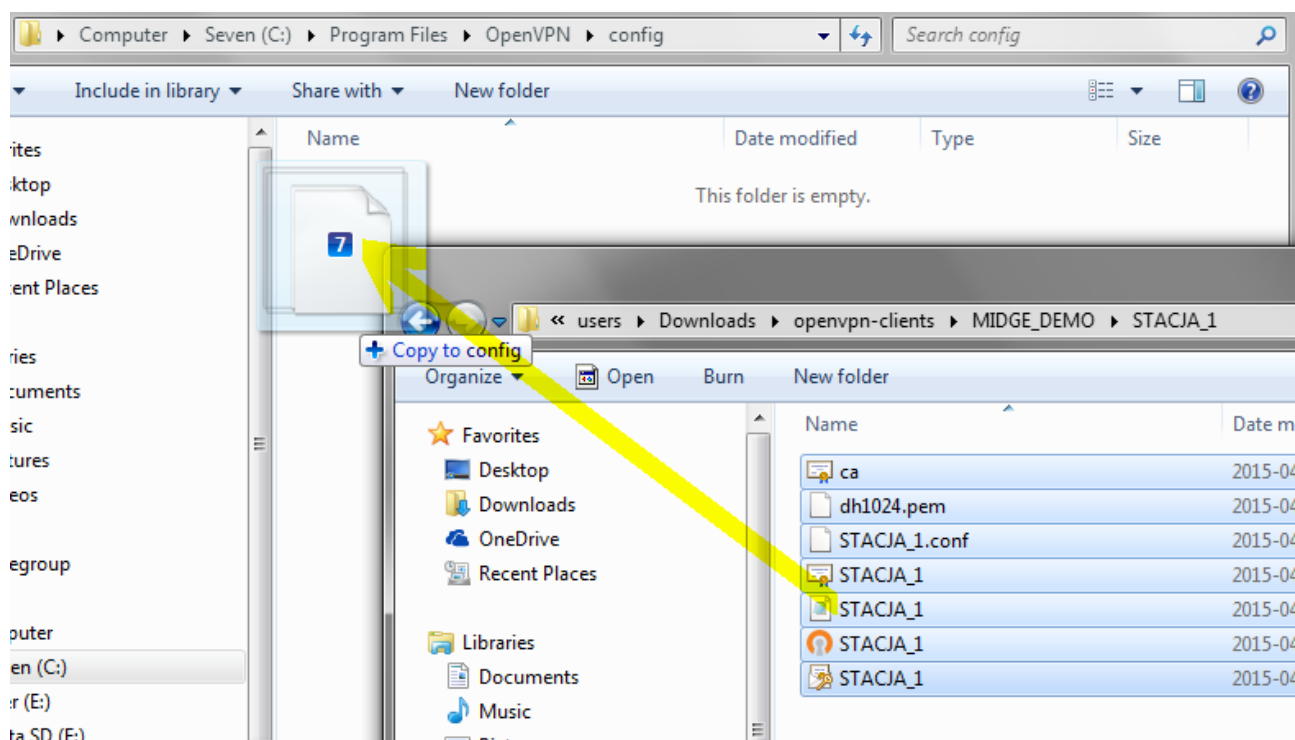
```
C:\Users\Serwis>
```

KONFIGURACJA KLIENTA TAP/TUN DLA WINDOWS

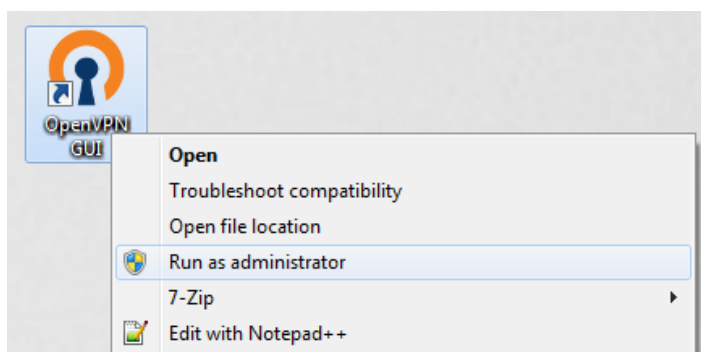
Do obsługi interfejsu TUN/TAP na komputerach PC użyj aplikacji z oryginalnego pakietu oprogramowania OpenVPN. Program najlepiej pobrać ze strony <http://openvpn.net/index.php/download/community-downloads.html>, zgodnie z wersją posiadanego systemu operacyjnego.


Po instalacji pojawi się nowa ikona **OpenVPN GUI**. Zanim uruchomimy usługę, należy skonfigurować połączenie. W tym celu z archiwum *openvpn-clients.zip* należy wyodrębnić pliki z archiwów STACJA_1.zip, STACJA_2.zip.

Następnie na dysku systemowym należy odszukać katalog instalacyjny programu i folder *config*, (C:\Program Files\OpenVPN\config) i skopiuj pliki konfiguracyjne Klienta OpenVPN.



Po przeniesieniu plików uruchom aplikację OpenVPN GUI jako **Administrator**. Aplikacja w trybie użytkownika nie będzie w stanie uzupełnić tablicy routingu (w trybie TUN) lub poprawnie skonfigurować wirtualnej karty sieciowej (TAP). Pamiętaj, aby zezwolić zaporze **Firewall** na komunikację przez aplikację OpenVPN lub dopisać ją ręcznie do zaufanych.



Jeżeli tunel nie połączy się automatycznie, to odszukaj w zasobniku systemowym ikonę  i kliknij na nią dwukrotnie. Klienta OpenVPN możesz uruchomić również w trybie usługi (start automatyczny). W tym celu zapoznaj się z dokumentacją oprogramowania.

Lista zmian:

07.04.2015 utworzenie dokumentu - wersja 1.0