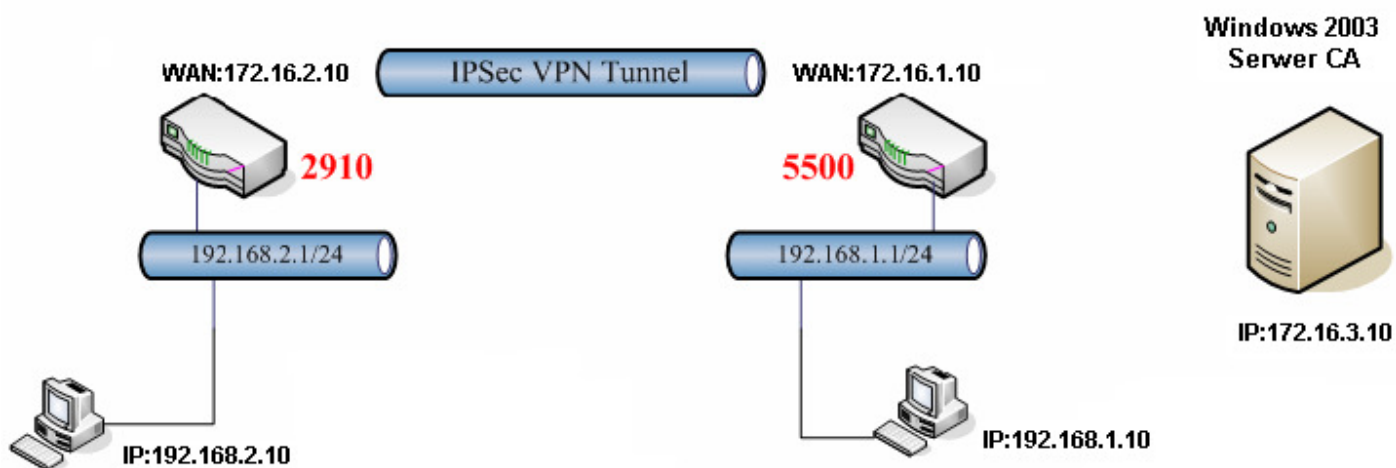


Zestawienie tunelu VPN po protokole IPSec pomiędzy routerem Vigor 2910 (klient VPN) a VigorPro 5500 (serwer VPN).

1. Certyfikaty na routerach Vigor
 - 1.1. Ustawienie czasu
 - 1.2. Lokalny certyfikat (żądanie certyfikatu z serwera CA)
 - 1.3. Certyfikat zaufanego CA
2. Konfiguracja serwera VPN
3. Konfiguracja klienta VPN
4. Status połączenia

Procedura konfiguracji została oparta na poniższym przykładzie.



Główne założenia:

- typ tunelu: LAN-LAN z routingiem pomiędzy podsieciami
- protokół VPN: IPSec
- szyfrowanie: AES
- integralność: SHA1 lub MD5
- autentykacja: certyfikaty X.509
- różne adresacje LAN:
 - serwer VPN: 192.168.1.1 /24
 - klient VPN: 192.168.2.1 /24

Uwaga!

Wymagane są różne adresacje sieci lokalnych

1. Certyfikaty na routerach Vigor

Uwaga!!! Poniższe kroki wykonaj zarówno dla Vigor 2910 jak i VigorPro 5500.

1.1. Ustawienie czasu

Ustaw aktualny czas na Vigorze, gdyż będzie on niezbędny do poprawnej pracy z certyfikatami X.509.

System >> Czas i data

Informacje o czasie

Aktualny stan zegara: 2008 Apr 1 Tue 11:5:0 Pobierz teraz

Ustawienia czasu

Pobierz z komputera
 Użyj serwera czasu

Protokół: NTP (RFC-1305)

Adres IP serwera: pool.ntp.org

Strefa czasowa: (GMT) Greenwich Mean Time : Dublin

Uwzględnij 1h przesunięcie czasu (zimowy/letni):

Okres uaktualniania: 30 min

1.2. Lokalny certyfikat (żądanie certyfikatu z serwera CA)

Krok 1: Przejdź do zakładki **Certyfikaty>>Lokalny certyfikat**. Następnie kliknij przycisk **GENERUJ**.

Certyfikaty >> Lokalny certyfikat

Ustawienia lokalnego certyfikatu X509

Nazwa	Podmiot	Stan	Modyfikuj
Lokalny	---	---	Pokaż Usuń

GENERUJ IMPORTUJ ODŚWIEŻ

Lokalny certyfikat X.509

Krok 2: Wpisz odpowiednie dane w polach **Alternatywna nazwa podmiotu** i **Nazwa podmiotu**. W przykładzie użyto wartości pokazanych na następnym rysunku. Po wprowadzeniu danych kliknij przycisk **Generuj**.

Certyfikaty >> Lokalny certyfikat

Generuj prośbę o certyfikat

Alternatywna nazwa podmiotu	
Type	Brak
Nazwa podmiotu	
Kraj (C)	PL
Stan (ST)	
Lokalizacja (L)	
Organizacja (O)	
Jednostka organizacyjna (OU)	
Podmiot (CN)	vigor
Email (E)	
Typ klucza	
	RSA
Rozmiar klucza	
	1024 Bit

Generuj

Krok 3: Wygenerowany tekst będzie potrzebny w kroku 7.

Certyfikaty >> Lokalny certyfikat

Ustawienia lokalnego certyfikatu X509

Nazwa	Podmiot	Stan	Modyfikuj
Lokalny	/C=PL/CN=vigor	Requesting	<input type="button" value="Pokaż"/> <input type="button" value="Usuń"/>

Prośba o certyfikat X509

```

-----BEGIN CERTIFICATE REQUEST-----
MIIBXDCBxgIBADAdMQswCQYDVQQGEwJQTEDEOMAwGA1UEAxMFdm1nb3IwgZ8wDQYJ
KoZInvcNAQEBBQADgYOAAMIGJAoGBA0j0GS1xyAI1YD3od8xHhcXfV6FDPFMDMWV
ZKwPCEviHhViWw7pJAspy/8eL8chlbeP3D082STwJvuvocVCrFk/5+DMwn2AaarnA
xkkG/eT1fNBoFVQ+u8K/gz/wcj2Jz2AeCuJrtW1ABvoxUWm84KHHCBF4egyNLLpn
635PFKB7AgMBAAGgADANBgkqhkiG9w0BAQUFAAOBgQCjokDh1UVhmrvDfIt1qyJI
pzKo0SaSgH77TK5elm+gMrxTlYjBKndmf3OqUoSg6Z4HUGMvmzQ2kQkQnenB9yK
8Uk1dRe9X0YQQKnTO54svuAPyAm1eCwdUo3BBSjBfnSwyaAJRUffdaAwaKBwaBt3
tanmg91rAqRWhYvUWbCSjw==
-----END CERTIFICATE REQUEST-----
    
```

Krok 4. Połącz się z serwerem CA (w przykładzie <http://172.16.3.10/certsrv>). W przykładzie wykorzystano Windows Server 2003 RC2 jako serwer CA. Po zalogowaniu wybierz **Żądanie certyfikatu**.

Zapraszamy

Użyj tej witryny sieci Web, aby zażądać certyfikatu dla tej przeglądarki sieci Web, klienta e-mail lub innego programu. Używając certyfikatu możesz potwierdzać swoją tożsamość w komunikacji z innymi osobami przez sieć Web, podpisywać i szyfrować wiadomości oraz, w zależności od typu żądanego certyfikatu, wykonywać inne zadania zabezpieczeń.

Możesz także użyć tej witryny sieci Web, aby pobrać certyfikat urzędu certyfikacji, łańcuch certyfikatów, listę odwołań certyfikatów lub wyświetlić stan wykonywanego żądania.

Aby uzyskać więcej informacji o usługach certyfikatów, zobacz [dokumentację usług certyfikatów](#).

Wybierz zadanie:

[Żądanie certyfikatu](#)

[Pokaż stan oczekującego żądania certyfikatu](#)

[Pobierz certyfikat urzędu certyfikacji, łańcuch certyfikatów lub listę CRL](#)

Krok 5: Wybierz **zaawansowane żądanie certyfikatu**.

Usługi certyfikatów *Microsoft* -- brinet Strona główna

Żądaj certyfikatu

Wybierz typ certyfikatu:
[Certyfikat użytkownika](#)

Możesz też przesłać [zaawansowane żądanie certyfikatu](#).

Krok 6: Wybierz drugą opcję – **Prześlij żądanie certyfikatu, używając ...**

Usługi certyfikatów *Microsoft* -- brinet Strona główna

Zaawansowane żądanie certyfikatu

Zasady tego urzędu certyfikacji decydują o typach certyfikatów, jakich możesz żądać. Kliknij jedną z poniższych opcji:

[Utwórz i prześlij żądanie do tego urzędu certyfikacji.](#)

[Prześlij żądanie certyfikatu, używając pliku CMC lub PKCS #10 szyfrowanego algorytmem base-64 lub prześlij żądanie odnowienia, używając pliku PKCS #7 szyfrowanego algorytmem base-64.](#)

[Zażądaj certyfikatu dla karty inteligentnej w imieniu innego użytkownika, korzystając ze stacji rejestrowania certyfikatów kart inteligentnych.](#)

Uwaga: aby przesłać żądanie w imieniu innego użytkownika, musisz mieć certyfikat agenta rejestrowania.

Krok 7. Wklej tekst wygenerowany w kroku 3. Wybierz opcję **Router (żądanie offline)** jako Szablon certyfiaktu. Następnie kliknij przycisk **Prześlij>**.

Usługi certyfikatów *Microsoft* -- brinet Strona główna

Prześlij żądanie certyfikatu lub odnowienie żądania

Aby przesłać zapisane żądanie do urzędu certyfikacji, w polu Zapisane żądanie wklej żądanie certyfikatu CMC lub PKCS #10 szyfrowane algorytmem base-64 lub żądanie odnowienia PKCS #7 wygenerowane przez źródło zewnętrzne (takie jak serwer sieci Web).

Zapisane żądanie:

Żądanie certyfikatu szyfrowanego algorytmem Base-64 (CMC lub PKCS #10 lub PKCS #7):

```

xkkG/eT1fNBofVQ+u8K/gz/wcj2Jz2AeCuJRtW1A
635FFKB7AgMBAAGgADANBgkqhkiG9w0BAQUFAAOB
pzKo0SaSgH77TK5elm+gMrxT1YjBKcndmf3OqUoS
8Uk1dRe9X0YQQKnTOS4svuAFyAm1eCwdUo3BsBsj
tanmg91rAqRWhYvUWbCSjw==
-----END CERTIFICATE REQUEST-----
    
```

[Przełóżaj w poszukiwaniu pliku do wstawienia.](#)

Szablon certyfikatu:

Atrybuty dodatkowe:

Atrybuty:

Krok 8: Pobierz certyfikat szyfrowany algorytmem Base-64

Usługi certyfikatów *Microsoft* -- brinet Strona główna

Certyfikat został wystawiony

Żądany certyfikat został wystawiony.

Szyfrowany algorytmem DER lub Szyfrowany algorytmem Base-64

[Pobierz certyfikat](#)
[Pobierz łańcuch certyfikatów](#)

Krok 9: Zaimportuj lokalny certyfikat do Vigora – wybierz ścieżkę do certyfikatu i kliknij przycisk **Importuj**.

Certyfikaty >> Lokalny certyfikat

Import lokalnego certyfikatu X.509

Wybierz certyfikat lokalny.

C:\Documents and Settings\vigor\

Kliknij **Importuj** aby pobrać lokalny certyfikat.

Krok 10: Pomyślna próba importu certyfikatu.

Certyfikaty >> Lokalny certyfikat

Import certyfikatu X.509

Gratulacje!

Certyfikat lokalny został zaimportowany pomyślnie.

Kliknij aby przejrzeć certyfikat.

Aby zobaczyć certyfikat kliknij przycisk **Pokaż**.

Certyfikaty >> Lokalny certyfikat

Ustawienia lokalnego certyfikatu X509

Nazwa	Podmiot	Stan	Modyfikuj
Lokalny	/C=PL/CN=vigor	OK	<input type="button" value="Pokaż"/> <input type="button" value="Usuń"/>

Informacja o certyfikacie - Windows Internet Explorer

http://192.168.2.1/doc/XLoCFvi.htm

Informacja o certyfikacie

Nazwa :	Lokalny
Wydawca :	/DC=pl/DC=brinet/CN=brinet
Podmiot :	/C=PL/CN=vigor
Alternatywna nazwa podmiotu :	
Ważny od :	Apr 1 09:04:06 2008 GMT
Ważny do :	Apr 1 09:04:06 2010 GMT

1.3. Certyfikat zaufanego CA

Krok 1: Połącz się z serwerem CA (w przykładzie <http://172.16.3.10/certsrv>). Po zalogowaniu wybierz **Pobierz certyfikat urzędu certyfikacji, łańcuch certyfikatów lub listę CRL**.

Usługi certyfikatów Microsoft -- brinet Strona główna

Zapraszamy

Użyj tej witryny sieci Web, aby zażądać certyfikatu dla tej przeglądarki sieci Web, klienta e-mail lub innego programu. Używając certyfikatu możesz potwierdzać swoją tożsamość w komunikacji z innymi osobami przez sieć Web, podpisywać i szyfrować wiadomości oraz, w zależności od typu żądanego certyfikatu, wykonywać inne zadania zabezpieczeń.

Możesz także użyć tej witryny sieci Web, aby pobrać certyfikat urzędu certyfikacji, łańcuch certyfikatów, listę odwołań certyfikatów lub wyświetlić stan wykonywanego żądania.

Aby uzyskać więcej informacji o usługach certyfikatów, zobacz [dokumentację usług certyfikatów](#).

Wybierz zadanie:
[Żądanie certyfikatu](#)
[Pokaż stan oczekującego żądania certyfikatu](#)
[Pobierz certyfikat urzędu certyfikacji, łańcuch certyfikatów lub listę CRL](#)

Krok 2: Wybierz odpowiedni certyfikat urzędu certyfikacji (w przykładzie brinet) oraz **Base 64** jako Metodę kodowania. Następnie wybierz opcję **Pobierz certyfikat urzędu certyfikacji** i zapisz na dysku.

Usługi certyfikatów Microsoft -- brinet Strona główna

Pobierz certyfikat urzędu certyfikacji, łańcuch certyfikatów lub listę CRL

Do ufania certyfikatом wystawionym przez ten urząd certyfikacji, [zainstaluj jego łańcuch certyfikatów](#).

Aby pobrać certyfikat urzędu certyfikacji, łańcuch certyfikatów lub listę CRL, wybierz certyfikat i metodę kodowania.

Certyfikat urzędu certyfikacji:

Metoda kodowania:

DER
 Base 64

[Pobierz certyfikat urzędu certyfikacji](#)
[Pobierz łańcuch certyfikatów urzędu certyfikacji](#)
[Pobierz najnowszą podstawową listę CRL](#)
[Pobierz najnowszą różnicową listę CRL](#)

Krok 3: Przejdź do zakładki **Certyfikaty >> Certyfikat zaufanego CA**. Następnie kliknij przycisk **IMPORTUJ**.

Certyfikaty >> Certyfikat zaufanego CA

Tożsamości zaufanych CA (certyfikaty X.509)

Nazwa	Podmiot	Stan	Modyfikuj	
CA-1	---	---	<input type="button" value="Pokaż"/>	<input type="button" value="Usuń"/>
CA-2	---	---	<input type="button" value="Pokaż"/>	<input type="button" value="Usuń"/>
CA-3	---	---	<input type="button" value="Pokaż"/>	<input type="button" value="Usuń"/>

Krok 4: Wskaż ścieżkę z certyfikatem zaufanego CA. Następnie kliknij przycisk **Importuj**.

Certyfikaty >> Certyfikat CA

Importuj certyfikat urzędu certyfikacji (CA)

Wybierz certyfikat zaufanego CA.

C:\Documents and Settings\vigor\

Kliknij **Importuj** aby importować certyfikat do routera.

Krok 5: Pomyślna próba importu certyfikatu.

Certyfikaty >> Tożsamość urzędu certyfikacji CA

Import certyfikatu CA

Gratulacje!

Certyfikat CA został pomyślnie załadowany do routera.

Kliknij aby zobaczyć certyfikat.

2. Konfiguracja serwera VPN (5500)

Włączenie obsługi IPSec

Przejdź do zakładki **VPN i Dostęp Zdalny>>Protokoły VPN** w panelu konfiguracyjnym routera i sprawdź (lub zaznacz) czy jest włączona obsługa protokołu IPSec. Domyślnie włączona jest obsługa protokołów PPTP, IPSec i L2TP.

VPN i Dostęp Zdalny>> Protokoły VPN

Protokoły VPN

<input checked="" type="checkbox"/>	Włącz obsługę PPTP
<input checked="" type="checkbox"/>	Włącz obsługę IPSec
<input checked="" type="checkbox"/>	Włącz obsługę L2TP
<input type="checkbox"/>	Włącz dostęp ISDN

Konfiguracja identyfikatora IPSec

Przejdź do zakładki **VPN i Dostęp Zdalny>>Identyfikatory IPSec**. Stwórz odpowiedni profil (w przykładzie użyto profilu nr 1). W przykładzie użyto wartości pokazanych na następnym rysunku. Po wprowadzeniu danych kliknij przycisk **OK**.

VPN i Dostęp Zdalny>> Identyfikatory IPSec

Numer Profilu : 1

Nazwa profilu	2910
<input checked="" type="checkbox"/> Włącz	
<input type="radio"/> Akceptuj dowolny certyfikat	
<input type="radio"/> Akceptuj tylko certyfikaty wystawione dla:	
Typ	Adres IP
<input checked="" type="radio"/> Akceptuj tylko certyfikaty wystawione dla podmiotu spełniającego poniższe kryteria:	
Kraj (C)	PL
Stan (ST)	
Lokalizacja (L)	
Organizacja (O)	
Jednostka organizacyjna (OU)	
Podmiot (CN)	vigor
E-Mail (E)	

Konfiguracja profilu LAN-LAN

Przejdź do zakładki **VPN i Dostęp Zdalny >> Połączenia LAN-LAN**. Stwórz profil do obsługi tunelu (w przykładzie użyto konta nr 1) i wpisz odpowiednie dane.

Konfiguracja części **Ustawienia ogólne** zgodna z założeniami przykładu:

- wpisz dowolną nazwę profilu
- zaznacz **Włącz profil**
- jako kierunek inicjacji wybierz **Dial-In**
- ustaw **czas nieaktywności 0**, gdy połączenie ma być aktywne cały czas.

1. Ustawienia ogólne

Nazwa profilu: <input type="text" value="od2910"/>	Kierunek inicjacji: <input type="radio"/> Oba <input type="radio"/> Dial-Out <input checked="" type="radio"/> Dial-In
<input checked="" type="checkbox"/> Włącz profil	<input type="checkbox"/> Zawsze aktywne
Połączenie VPN przez: <input type="text" value="WAN1 najpiew"/>	<input type="checkbox"/> Czas nieaktywności: <input type="text" value="0"/> sek
Nazwy NetBIOS: <input checked="" type="radio"/> Przepuść <input type="radio"/> Blokuj	<input type="checkbox"/> Użyj PING dla podtrzymania
	PING na IP: <input type="text"/>

Konfiguracja części **Ustawienia Dial-In** zgodna z założeniami przykładu:

- w polu Protokół dla połączenia wybierz **Tunel IPSec**
- zaznacz **Określ Zdalna brama VPN**, a w polu **IP zdalnego serwera** wpisz adres IP routera – klienta VPN. W przykładzie użyto adresu IP 172.16.2.10
- w polu Tryb uwierzytelniania IKE wybierz **Podpis cyfrowy (cert. X.509)** i odpowiedni certyfikat. W przykładzie użyto '2910'
- w polu Poziom zabezpieczeń IPSec wybierz **AES**.

3. Ustawienia Dial-In (odbiór wywołania z innego routera)

Akceptowane protokoły <input checked="" type="checkbox"/> ISDN <input type="checkbox"/> PPTP <input checked="" type="checkbox"/> Tunel IPSec <input type="checkbox"/> L2TP z polisą IPSec <input type="text" value="Brak"/>	Użytkownik: <input type="text" value="???"/> Hasło: <input type="text"/> Kompresja VJ: <input checked="" type="radio"/> Włącz <input type="radio"/> Wyłącz
<input checked="" type="checkbox"/> Określ Zdalna brama VPN IP zdalnego serwera: <input type="text" value="172.16.2.10"/> lub ID: <input type="text"/>	Tryb uwierzytelniania IKE <input type="checkbox"/> Klucz IKE Klucz IKE: <input type="text"/> <input checked="" type="checkbox"/> Podpis cyfrowy (cert. X.509) <input type="text" value="2910"/>
	Poziom zabezpieczeń IPSec <input type="checkbox"/> Średni(AH) Wysoki(ESP) <input type="checkbox"/> DES <input type="checkbox"/> 3DES <input checked="" type="checkbox"/> AES

Konfiguracja części **Adresacja i routing oraz NAT wewnątrz połączenia** zgodna z założeniami przykładu:

- w przykładzie Zdalna podsieć: 192.168.2.0, Maska podsieci zdalnej: 255.255.255.0

4. Adresacja i routing oraz NAT wewnątrz połączenia

Własny WAN IP: <input type="text" value="0.0.0.0"/>	RIP dla VPN: <input type="text" value="Wyłącz"/>
IP zdalnej bramy: <input type="text" value="0.0.0.0"/>	Z lokalnej podsieci do zdalnej podsieci, wykonaj: <input type="text" value="Routing"/>
<input checked="" type="checkbox"/> IP zdalnej podsieci: <input type="text" value="192.168.2.0"/>	<input type="checkbox"/> Zmień trasę domyślną do tego tunelu VPN (Tylko dla pojedynczego WANu)
<input checked="" type="checkbox"/> Maska zdalnej podsieci: <input type="text" value="255.255.255.0"/>	
<input type="button" value="Więcej podsieci"/>	

Uwaga!!!

W niektórych modelach dostępne są dodatkowe pola określające IP lokalnej podsieci oraz jej maskę. Poniżej konfiguracja zgodna z założeniami przykładu.

IP zdalnej podsieci	<input type="text" value="192.168.2.0"/>
Maska zdalnej podsieci	<input type="text" value="255.255.255.0"/>
IP lokalnej podsieci	<input type="text" value="192.168.1.1"/>
Maska lokalnej podsieci	<input type="text" value="255.255.255.0"/>

3. Konfiguracja klienta VPN (2910)

Włączenie obsługi IPSec

Przejdź do zakładki **VPN i Dostęp Zdalny>>Protokoły VPN** w panelu konfiguracyjnym routera i sprawdź (lub zaznacz) czy jest włączona obsługa protokołu IPSec. Domyślnie włączona jest obsługa protokołów PPTP, IPSec i L2TP.

VPN i Dostęp Zdalny>> Protokoły VPN

Protokoły VPN

<input checked="" type="checkbox"/>	Włącz obsługę PPTP
<input checked="" type="checkbox"/>	Włącz obsługę IPSec
<input checked="" type="checkbox"/>	Włącz obsługę L2TP
<input type="checkbox"/>	Włącz dostęp ISDN

Konfiguracja identyfikatora IPSec

Przejdź do zakładki **VPN i Dostęp Zdalny>>Identyfikatory IPSec**. Stwórz odpowiedni profil (w przykładzie użyto profilu nr 1). W przykładzie użyto wartości pokazanych na następnym rysunku. Po wprowadzeniu danych kliknij przycisk **OK**.

VPN i Dostęp Zdalny>> Identyfikatory IPSec

Numer Profilu : 1

Nazwa profilu	5500
<input checked="" type="checkbox"/> Włącz	
<input type="radio"/> Akceptuj dowolny certyfikat	
<input type="radio"/> Akceptuj tylko certyfikaty wystawione dla:	
Typ	Adres IP
IP	
<input checked="" type="radio"/> Akceptuj tylko certyfikaty wystawione dla podmiotu spełniającego poniższe kryteria:	
Kraj (C)	PL
Stan (ST)	
Lokalizacja (L)	
Organizacja (O)	
Jednostka organizacyjna (OU)	
Podmiot (CN)	vigor
E-Mail (E)	

Konfiguracja profilu LAN-LAN

Przejdź do zakładki **VPN i Dostęp Zdalny**>>**Połączenia LAN-LAN**. Stwórz profil do obsługi tunelu (w przykładzie użyto konta nr 1) i wpisz odpowiednie dane.

Konfiguracja części **Ustawienia ogólne** zgodna z założeniami przykładu:

- wpisz dowolną nazwę profilu
- zaznacz **Włącz profil**
- jako kierunek inicjacji wybierz **Dial-Out**
- zaznacz **Zawsze aktywne** - w ten sposób ustawisz **czas nieaktywności -1**, gdy połączenie ma być aktywne cały czas.

1. Ustawienia ogólne

Nazwa profilu <input type="text" value="do 5500"/>	Kierunek inicjacji <input type="radio"/> Oba <input checked="" type="radio"/> Dial-Out <input type="radio"/> Dial-In
<input checked="" type="checkbox"/> Włącz profil	<input checked="" type="checkbox"/> Zawsze aktywne
Połączenie VPN przez: <input type="text" value="WAN1 najpierw"/>	Czas nieaktywności <input type="text" value="-1"/> sek
	<input type="checkbox"/> Użyj PING dla podtrzymania
	PING na IP <input type="text"/>

Konfiguracja części **Ustawienia Dial-Out** zgodna z założeniami przykładu:

- w polu Protokół dla połączenia wybierz **Tunel IPSec**
- w polu **IP/nazwa DNS serwera VPN** wpisz adres IP routera, do którego zestawiasz tunnel VPN, albo jego nazwę. W przykładzie adres IP 172.16.1.10
- w polu Tryb uwierzytelniania IKE wybierz **Podpis cyfrowy (cert. X.509)** i odpowiedni certyfikat. W przykładzie użyto '5500'
- w polu Poziom zabezpieczeń IPSec wybierz protokół realizujący szyfrowanie i uwierzytelnianie **Wysoki(ESP)**. W przykładzie użyto AES z autentykacją SHA1/MD5

2. Ustawienia Dial-Out (inicjacja do innego routera)

Protokół dla połączenia <input type="radio"/> ISDN <input type="radio"/> PPTP <input checked="" type="radio"/> Tunel IPSec <input type="radio"/> L2TP z polisą IPSec <input type="text" value="Brak"/>	Typ łącza ISDN <input type="text" value="64k bps"/> Użytkownik <input type="text" value="???"/> Hasło <input type="text"/> Uwierzytelnianie PPP <input type="text" value="PAP/CHAP"/> Kompresja VJ <input checked="" type="radio"/> Włącz <input type="radio"/> Wyłącz
Numer docelowy (dla ISDN) IP/nazwa DNS serwera VPN. (np. 5551234, draytek.com lub 123.45.67.89) <input type="text" value="172.16.1.10"/>	Tryb uwierzytelniania IKE <input type="radio"/> Klucz IKE <input checked="" type="radio"/> Podpis cyfrowy (cert. X.509) <input type="text" value="5500"/>
	Poziom zabezpieczeń IPSec <input type="radio"/> Średni(AH) <input checked="" type="radio"/> Wysoki (ESP) <input type="text" value="AES z autentykacją"/> <input type="button" value="Zaawansowane"/>

Konfiguracja części **Adresacja i routing oraz NAT wewnątrz połączenia** zgodna z założeniami przykładu:

- w przykładzie Zdalna podsieć: 192.168.1.0, Maska podsieci zdalnej: 255.255.255.0

4. Adresacja i routing oraz NAT wewnątrz połączenia

Własny WAN IP <input type="text" value="0.0.0.0"/>	RIP dla VPN <input type="text" value="Wyłącz"/>
IP zdalnej bramy <input type="text" value="0.0.0.0"/>	<input checked="" type="checkbox"/> Z lokalnej podsieci do zdalnej podsieci, wykonaj
<input checked="" type="checkbox"/> IP zdalnej podsieci <input type="text" value="192.168.1.0"/>	<input type="text" value="Routing"/>
<input checked="" type="checkbox"/> Maska zdalnej podsieci <input type="text" value="255.255.255.0"/>	<input type="checkbox"/> Zmień trasę domyślną do tego tunelu VPN (Tylko dla pojedynczego WANu)
<input type="button" value="Więcej podsieci"/>	

4. Status połączenia (od strony klienta VPN)

O tym, czy tunel został zainicjowany, możesz przekonać się wybierając **VPN i Dostęp Zdalny>>Zarządzanie połączeniem** (rysunek poniżej).

VPN i Dostęp Zdalny>> Zarządzanie połączeniem

Wymuszanie inicjacji połączeń Czas odświeżania : 10

Tryb Główny:	(do 5500) 172.16.1.10	<input type="button" value="Inicjuj"/>
Tryb Backup:		<input type="button" value="Inicjuj"/>

Stan połączenia VPN Nr strony

Bieżąca strona: 1

VPN	Typ	Zdalny IP	Sieć wirtualna	Tx pakietów	Tx predkość	Rx pakietów	Rx predkość	Czas
1	IPSec Tunnel (do 5500) AES-SHA1 Auth	172.16.1.10	192.168.1.0/24	61	60	63	60	0:1:4

xxxxxxx : Dane są szyfrowane.
xxxxxxx : nie są szyfrowane.

Inny sposób to np. zwykły ping. Wybierz Menu Start a następnie Uruchom i wpisz cmd . Następnie wykonaj polecenie: ping adres_hosta_w_LAN-ie (patrz rysunek poniżej, gdzie host posiada adres LAN-owy 192.168.1.10). Po zainicjowaniu tunelu otrzymasz poprawną odpowiedź na ping – świadczy ona o poprawnej komunikacji w tunelu VPN.

```
C:\>ping 192.168.1.10

Badanie 192.168.1.10 z użyciem 32 bajtów danych:

Odpowiedź z 192.168.1.10: bajtów=32 czas=3ms TTL=126
Odpowiedź z 192.168.1.10: bajtów=32 czas=3ms TTL=126
Odpowiedź z 192.168.1.10: bajtów=32 czas=3ms TTL=126
Odpowiedź z 192.168.1.10: bajtów=32 czas=3ms TTL=126

Statystyka badania ping dla 192.168.1.10:
    Pakiety: Wysłane = 4, Odebrane = 4, Utracone = 0 (0% strat),
Szacunkowy czas błędzenia pakietów w milisekundach:
    Minimum = 3 ms, Maksimum = 3 ms, Czas średni = 3 ms
```

Krzysztof Skowina
 Specjalista ds. rozwiązań sieciowych
 BRINET Sp. z o.o.
k.skowina@brinet.pl