

1. Czas
2. Harmonogram
3. Firewall
 - 3.1. Ustawienia ogólne
 - 3.2. Filtr danych

Założenia:

- 192.168.1.10 ma zablokowaną możliwość nawiązywania nowych połączeń z Internetem codziennie w godzinach 22:00-06:00

Uwaga!

Godziny reguł czasowych dotyczą doby (00:00-23:59). Użycie harmonogramu ze zmianą daty (23:59->00:00) wymaga dwóch reguł czasowych (XX:XX-23:59, 00:00-YY:YY).

1. Czas

Przejdź do zakładki **System>>Ustawienia Czasu** w panelu konfiguracyjnym routera. W przykładzie użyto serwera czasu. W tym celu wpisz serwer czasu np. pool.ntp.org, wybierz odpowiednią strefę czasową oraz zaznacz opcję uwzględniającą przesunięcie czasowe. Po wprowadzeniu danych kliknij przycisk OK.

System >> Ustawienia czasu

Informacje o czasie

Aktualny stan zegara	2011 Nov 16 Wed 13 : 0 : 55	<input type="button" value="Pobierz teraz"/>
----------------------	-----------------------------	--

Ustawienia czasu

<input type="radio"/> Użyj czasu przeglądarki	
<input checked="" type="radio"/> Użyj serwera czasu	
Adres IP serwera	<input type="text" value="pool.ntp.org"/>
Strefa czasowa	<input type="text" value="(GMT+01:00) Warsaw, Zagreb"/>
Uwzględniaj 1h przesunięcie czasu (zimowy/letni)	<input checked="" type="checkbox"/>
Okres uaktualniania	<input type="text" value="30 min"/>

2. Harmonogram

Przejdź do zakładki **Aplikacje i Usługi>>Harmonogram** w panelu konfiguracyjnym routera. Utwórz nową regułę czasową. Poniżej ustawienia zgodne z założeniami przykładu.

Aplikacje i Usługi >> Harmonogram

Indeks Nr. 1

<input checked="" type="checkbox"/> Włącz regułę czasową	
Data rozpoczęcia (rok-miec-dzien)	<input type="text" value="2000"/> - <input type="text" value="1"/> - <input type="text" value="1"/>
Czas rozpoczęcia (godz:min)	<input type="text" value="22"/> : <input type="text" value="0"/>
Czas trwania (godz:min)	<input type="text" value="2"/> : <input type="text" value="0"/>
Akcja	<input type="text" value="Wymuś natychmiast"/>
Czas nieaktywności	<input type="text" value="0"/> min. (maks. 255)
Jak często	
<input type="radio"/> Jednorazowo	
<input checked="" type="radio"/> Dni tygodnia	
<input checked="" type="checkbox"/> Nie	<input checked="" type="checkbox"/> Pon <input checked="" type="checkbox"/> Wt <input checked="" type="checkbox"/> Śr <input checked="" type="checkbox"/> Czw <input checked="" type="checkbox"/> Pt <input checked="" type="checkbox"/> So

Aplikacje i Usługi >> Harmonogram

Indeks Nr. 2

Włącz regułę czasową

Data rozpoczęcia (rok-mieć-dzień) 2000 - 1 - 1

Czas rozpoczęcia (godz:min) 0 : 0

Czas trwania (godz:min) 6 : 0

Akcja Wymuś natychmiast

Czas nieaktywności 0 min. (maks. 255)

Jak często

Jednorazowo

Dni tygodnia

Nie Pon Wt Śr Czw Pt So

3. Firewall

3.1. Ustawienia ogólne

Przejdź do zakładki **Firewall>>Ustawienia Ogólne** w panelu konfiguracyjnym routera.

Poniżej ustawienia zgodne z założeniami przykładu dla:

- **wszystkich hostów**: wybierz odpowiednie profile **Działanie dla domyślnej reguły**
- **PC w godzinach 22:00-06:00**: włącz **Filtr danych**, wybierz **Zestaw#2** oraz dokonaj konfiguracji opisanej w podpunkcie 3.2.

Firewall >> Ustawienia ogólne

Ustawienia ogólne

Filtr połączeń Włącz Zestaw startowy Zestaw#1

Wyłącz

Filtr danych Włącz Zestaw startowy Zestaw#2

Wyłącz

Działanie dla domyślnej reguły:

Zastosowanie	Działanie/Akcja	Syslog
Filtr	Przepuść	<input type="checkbox"/>
Filtr IMP2P	Brak	<input type="checkbox"/>
Filtr zawartości URL	Brak	<input type="checkbox"/>
Filtr treści Web	Brak	<input type="checkbox"/>

Ustawienia zaawansowane

Akceptuj przychodzące fragmenty pakietów UDP (dla niektórych gier, np. CS)

Kliknij przycisk **Edytuj**, aby edytować Ustawienia zaawansowane domyślnej reguły. Wybierz odpowiednią stronę kodową.

Firewall >> Ustawienia ogólne

Ustawienia zaawansowane

Strona kodowa ANSI(1250)-Central Europe

Rozmiar okna: 65535

Timeout sesji: 1440 Minut(y)

3.2. Filtr danych

Przejdź do zakładki **Firewall>>Filtr Pakietów** w panelu konfiguracyjnym routera. Wybierz zestaw reguł i stwórz właściwe reguły. W przykładzie dodano reguły filtru do domyślnego zestawu nr 2.

Firewall >> Ustawienia filtrów IP

Ustawienia filtrów IP | [Ustawienia domyślne](#) |

Zestaw	Komentarz	Zestaw	Komentarz
1.	Default Call Filter	7.	
2.	Default Data Filter	8.	
3.		9.	
4.		10.	
5.		11.	
6.		12.	

Stwórz odpowiednie reguły do filtrowania ruchu:

- Pierwsza reguła jest domyślna i służy do blokowania NetBios.
- Druga reguła jest wykorzystywana do blokowania możliwości nawiązywania nowych połączeń z Internetem przez PC codziennie w godzinach 22:00-06:00

Firewall >> Ustawienia filtru >> Edycja zestawu reguł

Zestaw filtru 2
Komentarz : Default Data Filter

Reguła filtru	Aktywne	Komentarz	Przesuń wyżej	Przesuń niżej
<input type="text" value="1"/>	<input checked="" type="checkbox"/>	xNetBios -> DNS		Niżej
<input type="text" value="2"/>	<input checked="" type="checkbox"/>	PC out	Wyżej	Niżej
<input type="text" value="3"/>	<input type="checkbox"/>		Wyżej	Niżej
<input type="text" value="4"/>	<input type="checkbox"/>		Wyżej	Niżej
<input type="text" value="5"/>	<input type="checkbox"/>		Wyżej	Niżej
<input type="text" value="6"/>	<input type="checkbox"/>		Wyżej	Niżej
<input type="text" value="7"/>	<input type="checkbox"/>		Wyżej	

Następny zestaw

Reguła 2

Blokowanie możliwości nawiązywania nowych połączeń z Internetem przez PC codziennie w godzinach 22:00-06:00
W polach Harmonogram wpisz numery utworzonych reguł czasowych.

[Firewall >> Edycja zestawu reguł > Edycja reguły](#)

Zestaw reguł 2 Reguła 2

<input checked="" type="checkbox"/> Zaznacz aby uaktywnić regułę		
Komentarz	PC out	
Reguły (1-15) z menu Harmonogram Ustawienia:	1, 2, ,	
Kierunek:	LAN->WAN	
Źródło:	192.168.1.10	
Przeznaczenie:	Any	
Typ usługi:	Any	
Fragmentacja:	Bez znaczenia	
Zastosowanie	Działanie/Akcja	SysLog
Filtr:	Zablokuj natychmiast	<input type="checkbox"/>
Skok na skrót do innego zestawu:	Brak	
Filtr IM/P2P:	Brak	<input type="checkbox"/>
Filtr zawartości URL	Brak	<input type="checkbox"/>
Filtr Treści Web	Brak	<input type="checkbox"/>
Ustawienia zaawansowane	Edytuj	

Uwaga!

Nowsze routery(firmware) wspierają możliwość czyszczenia sesji spełniających regułę firewall jeśli uruchomiony jest harmonogram. Dzięki tej opcji można zablokować istniejące już połączenia z Internetem.

Reguły (1-15) z menu Harmonogram Ustawienia:	1, 2, ,
Wyczyść sesje jeśli harmonogram WŁĄCZONY:	<input checked="" type="checkbox"/> Włącz