



Założenia:

 PC1 (192.168.1.11) ma zablokowaną możliwość nawiązywania nowych połączeń z Internetem codziennie w godzinach 22:00-06:00

Przejdź do zakładki **Object Settings>>IP Object**. Stwórz odpowiedni profil adresu IP.

Objec	ts Setting >> IP Object					6
	IP Object					
	🚯 Add 🔀 Edit 🛅 I	Delete 🔇 🐼 Refresh			Profile Number Limit	: 200
	Profile	Address Type	Start IP Address	End IP Address	Subnet Mask	
1	PC1	Single	192.168.1.11			

IP Object	- ×
Profile :	PC1
Address Type :	Single 🗸
Start IP Address :	192 . 168 . 1 . 11



Przejdź do zakładki **System Maintenance>>Time and Date**. Wybierz odpowiednią strefę czasową.

System Maintenance >> Time and Date					
Time and Date					
Time Type :	NTP	~			
Server:	pool.ntp.org 123				
Port :					
Interval :	600				
Time Zone :	Warsaw	٧			
Daylight Saving :	🌀 Enable 💿 Disable				

Przejdź do zakładki **Object Setting>>Time Object**. Stwórz odpowiedni profil czasu.

0	Jbjects Setting >> Time Object							
	Time Object							
🚯 Add 🔀 Edit 🍈 Delete 🔊 Refresh Profile Number Limit								
	Profile Frequen	uency Start Date	Start Time End Date	End Time	Weekdays			
	22_6 Weekdays	days 2014-01-01	10:00pm 2014-01-01	06:00am	Mon,Tue,Wed,Thu,Fri,Sat,Sun			

Time Object	-×
Profile :	22_6
Frequency :	Weekdays 👻
Start Date :	2014-01-01
Start Time :	Hour Min Sec 22 v 00 v 00 v
End Date :	2014-01-01
End Time :	Hour Min Sec 06 ¥ 00 ¥ 00 ¥
Weekdays :	Mon, Tue, Wed, Thu, Fr 👻



Przejdź do zakładki **Firewall>>Filter Setup>>IP Filter**. Stwórz odpowiednią grupę oraz regułę wybierając wcześniej stworzone profile.

	Add 🔀 Edit 🕅 Dele'	te 🔇 Refresh 🍲 Mi	ove Up 🛛 🐣 Move Down	n				Profile Number L
G	Group		Enable			Comment		
I PC	C1_filter		true					
	🚯 Add 🔀 Edit 🗻	Delete 🏈 Refresh 🄇	a Rename 🍲 Move	Up 😽 Move Down				Profile Number Limit : 2
Ru	ile Enable	Action	Next Group For F	Syslog	Source LDAP Gr.	General Firewall .	Source Firewall	Destination Fire
PC1	1_block true	block		Disable		22_6	PC1	
	Profile : PC1_block	k						
	V Enabl	le						
Blo	ock Action : Block	~						
Ne	ext Group :	~						
THE	ski oroup .	· · ·						
	SysLog : O Enab	ole o Disable						
put	Interface : ALL LAN	s v						
put	Interface : ALL WAN	vs v						
	target has been sper	rified firewall rules a	re applied to Apy of	hiect				
-		unca, mewairaica a	re applied to Airy of	bjoor				
F	irewall Objects							
Im	e Schedule							
Ti	me Object							
1	Profile	Frequency	Start Date	Start Time	End Date	End Time	Weekdays	Edit
V	/ 22_6	Weekdays	2014-01-01	10:00pm	2014-01-01	06:00am I	Non, Tue, Wed, T	···· 🗶
Ti	ime Group							
Son	vice Protocol							
	vice Protocol							
50	ervice Type Object							
Se	ervice Type Group							
nco	oming Country Filte	r						
S	ource Country Object	(At most accept 15 c	ountries)					
Dut-	-going Country Filte	er						
De	estination Country Ob	ject (At most accept	15 countries)					
Sou	Irce IP							
S	ource IP Object							
	Profile	Address Ty	pe Start I	P Address	End IP Addre	ss Subn	et Mask	Edit
V	PC1	Single	192.16	8.1.11				×
7	ource IP Group							
	ource llear Drofile							
Sc.	Juice User Profile							
So So	aurea llaar O							
So So So	ource User Group							
So So So	ource User Group ource LDAP Group							
So So So So So	ource User Group ource LDAP Group tination IP							
	ource User Group ource LDAP Group tination IP estination IP Object							
	ource User Group ource LDAP Group stination IP estination IP Object estination IP Group							
	ource User Group ource LDAP Group tination IP estination IP Object estination IP Group estination DNS Object	1						
	ource User Group ource LDAP Group stination IP estination IP Object estination IP Group estination DNS Object estination User Profile							

3/4



Przejdź do zakładki **Firewall>>Filter Setup>>Default Policy**. Domyślnie router przepuszcza ruch do Internetu, który nie spełnia kryteriów Filtru IP, Filtru Aplikacji, Filtru URL/Kategorii Web.

Fire	ewall >> Filter :	Setup >> Defaul	t Policy			
	IP Filter	IPv6 Filter	Application Filter	URL/Web Category Filter	QQ Filter	Default Policy
	Use Defaul	t Policy : Acce	pt	v		

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