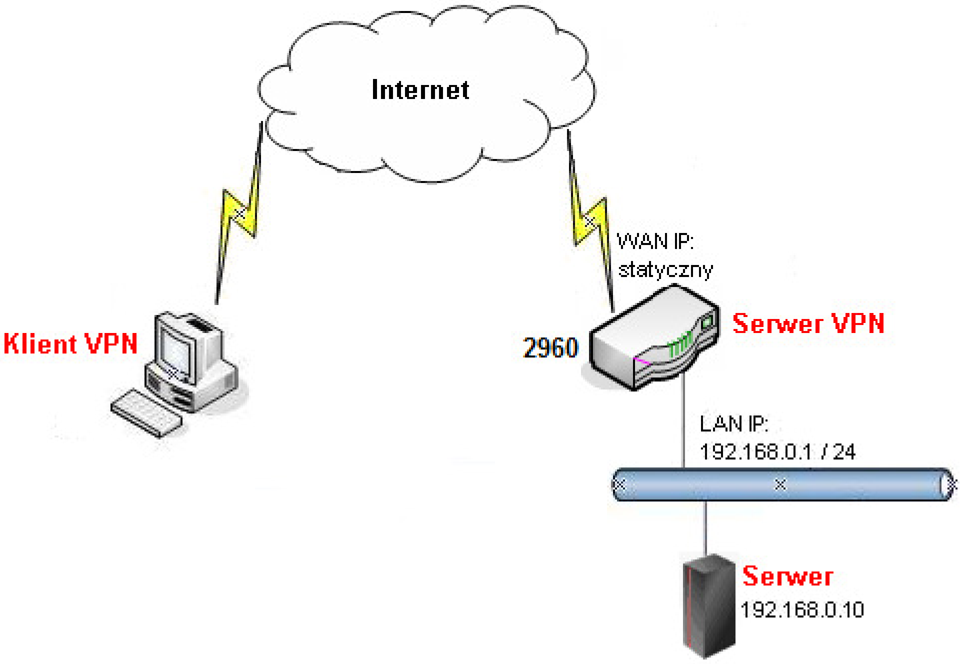
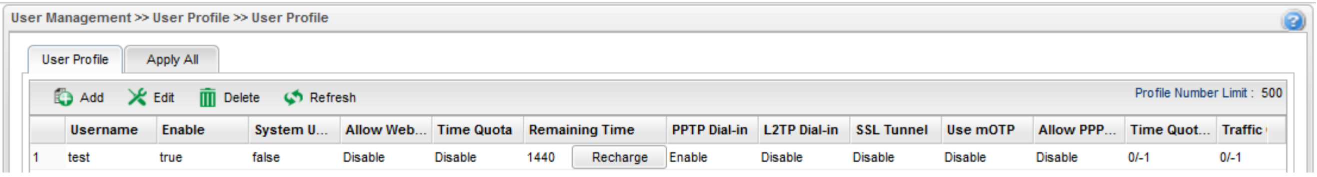


Główne założenia:

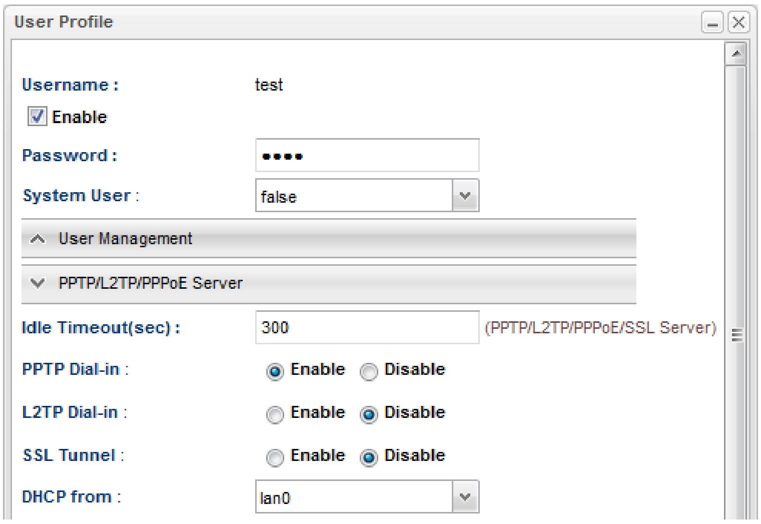
- PPTP Host-LAN
- Klient VPN ma dostęp tylko do Serwera 192.168.0.10 – brak dostęp do pozostałych urządzeń w podsieci 192.168.0.0/24

Przejdź do zakładki **User Management>>User Profile>>User Profile**. Stwórz odpowiedni profil użytkownika.



Profile Number Limit : 500

	Username	Enable	System U...	Allow Web...	Time Quota	Remaining Time	PPTP Dial-in	L2TP Dial-in	SSL Tunnel	Use mOTP	Allow PPP...	Time Quot...	Traffic
1	test	true	false	Disable	Disable	1440 Recharge	Enable	Disable	Disable	Disable	Disable	0/-1	0/-1



Username : test

☑ Enable

Password : ••••

System User : false

Idle Timeout(sec) : 300 (PPTP/L2TP/PPPoE/SSL Server)

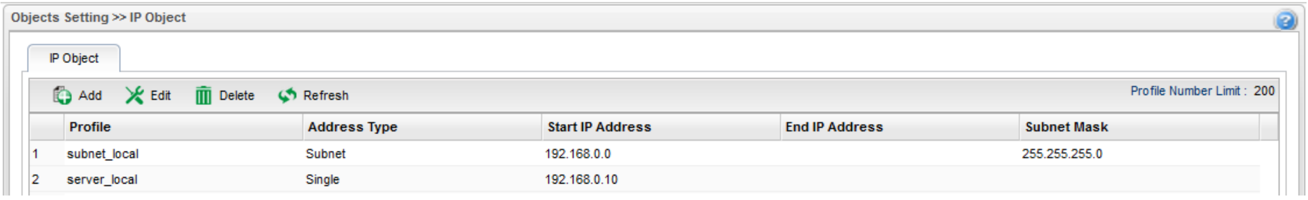
PPTP Dial-in : ● Enable ○ Disable

L2TP Dial-in : ○ Enable ● Disable

SSL Tunnel : ○ Enable ● Disable

DHCP from : lan0

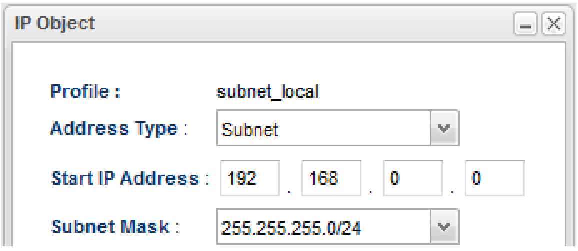
Przejdź do zakładki **Object Settings>>IP Object**. Stwórz odpowiednie profile adresów IP.



Objects Setting >> IP Object

Profile Number Limit : 200

	Profile	Address Type	Start IP Address	End IP Address	Subnet Mask
1	subnet_local	Subnet	192.168.0.0		255.255.255.0
2	server_local	Single	192.168.0.10		



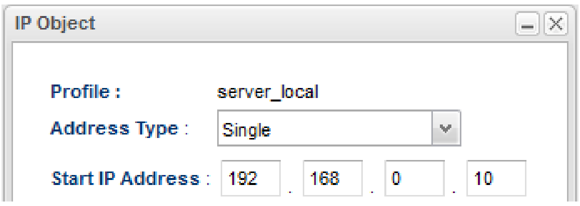
IP Object

Profile : subnet_local

Address Type : Subnet

Start IP Address : 192 . 168 . 0 . 0

Subnet Mask : 255.255.255.0/24



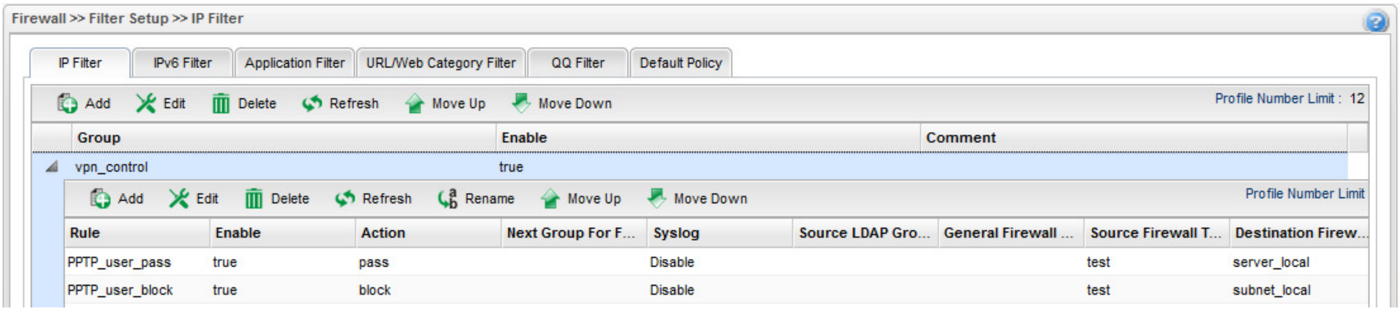
IP Object

Profile : server_local

Address Type : Single

Start IP Address : 192 . 168 . 0 . 10

Przejdź do zakładki **Firewall>>Filter Setup>>IP Filter**. Stwórz odpowiednią grupę oraz reguły wybierając wcześniej stworzone profile obiektów oraz profil użytkownika.



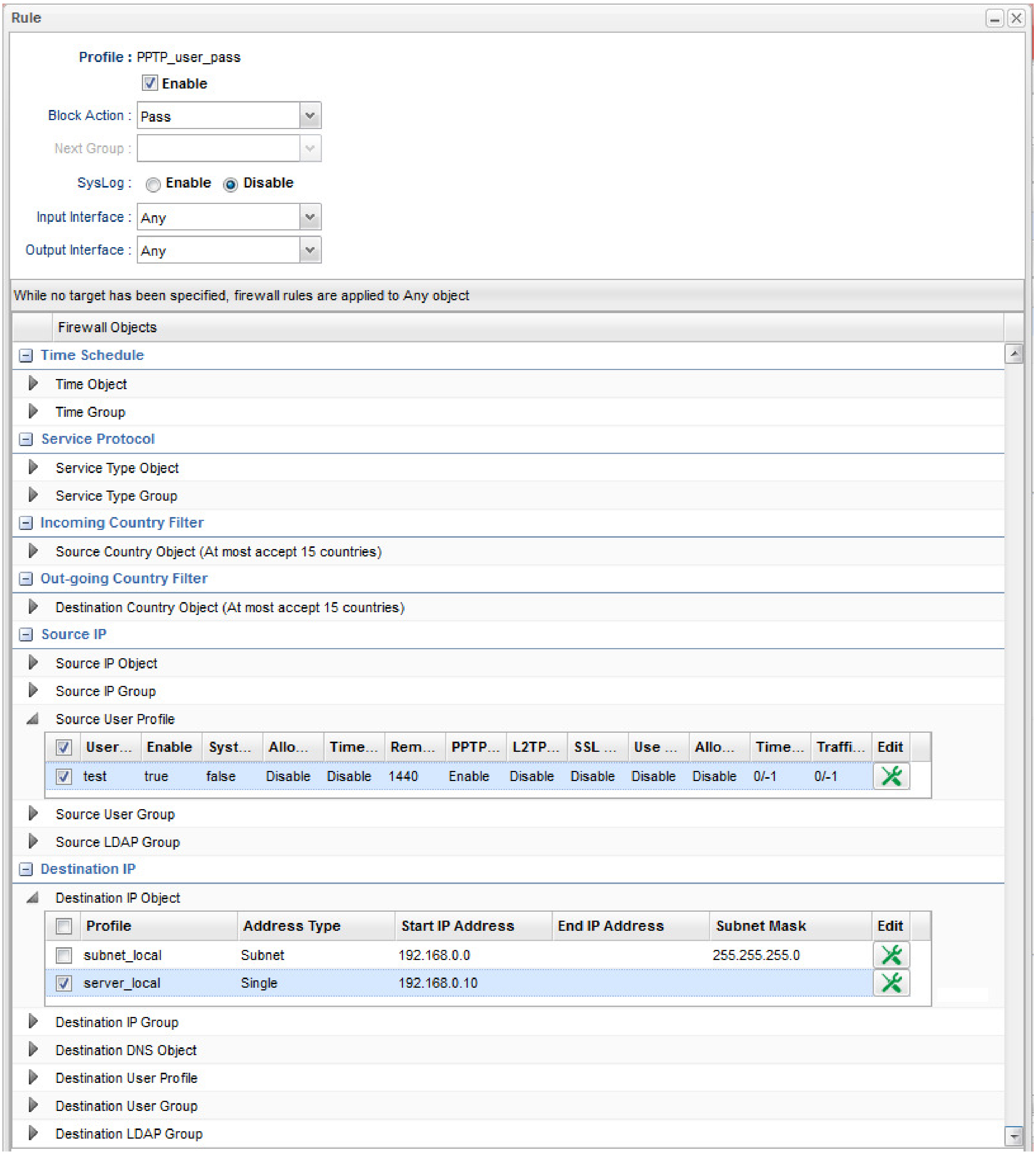
Firewall >> Filter Setup >> IP Filter

Profile Number Limit : 12

Group	Enable	Comment
vpn_control	true	

Profile Number Limit

Rule	Enable	Action	Next Group For F...	Syslog	Source LDAP Gro...	General Firewall ...	Source Firewall T...	Destination Firew...
PPTP_user_pass	true	pass		Disable			test	server_local
PPTP_user_block	true	block		Disable			test	subnet_local



Rule

Profile : PPTP_user_pass

☑ Enable

Block Action : Pass

Next Group :

SysLog : ○ Enable ● Disable

Input Interface : Any

Output Interface : Any

While no target has been specified, firewall rules are applied to Any object

Firewall Objects

⊟ Time Schedule

- Time Object
- Time Group

⊟ Service Protocol

- Service Type Object
- Service Type Group

⊟ Incoming Country Filter

- Source Country Object (At most accept 15 countries)

⊟ Out-going Country Filter

- Destination Country Object (At most accept 15 countries)

⊟ Source IP

- Source IP Object
- Source IP Group
- Source User Profile

☑	User...	Enable	Syst...	Allo...	Time...	Rem...	PPTP...	L2TP...	SSL ...	Use ...	Allo...	Time...	Traffi...	Edit
☑	test	true	false	Disable	Disable	1440	Enable	Disable	Disable	Disable	Disable	0/-1	0/-1	✎

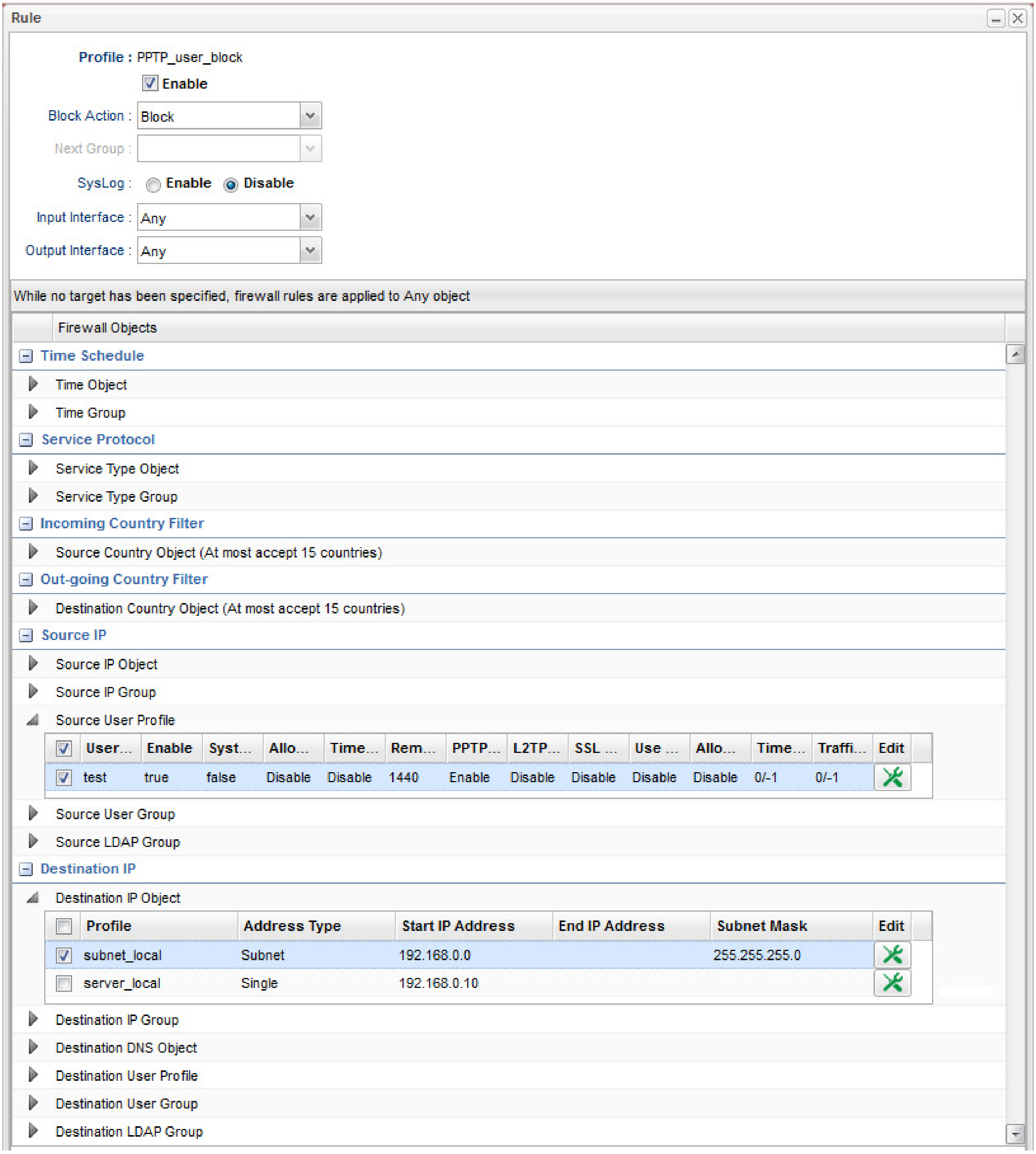
- Source User Group
- Source LDAP Group

⊟ Destination IP

- Destination IP Object

□	Profile	Address Type	Start IP Address	End IP Address	Subnet Mask	Edit
□	subnet_local	Subnet	192.168.0.0		255.255.255.0	✎
☑	server_local	Single	192.168.0.10			✎

- Destination IP Group
- Destination DNS Object
- Destination User Profile
- Destination User Group
- Destination LDAP Group



Rule

Profile : PPTP_user_block

☑ Enable

Block Action :	Block
Next Group :	
SysLog :	○ Enable ● Disable
Input Interface :	Any
Output Interface :	Any

While no target has been specified, firewall rules are applied to Any object

Firewall Objects

⊟ Time Schedule

- ▶ Time Object
- ▶ Time Group

⊟ Service Protocol

- ▶ Service Type Object
- ▶ Service Type Group

⊟ Incoming Country Filter

- ▶ Source Country Object (At most accept 15 countries)

⊟ Out-going Country Filter

- ▶ Destination Country Object (At most accept 15 countries)

⊟ Source IP

- ▶ Source IP Object
- ▶ Source IP Group
- ◢ Source User Profile

☑	User...	Enable	Syst...	Allo...	Time...	Rem...	PPTP...	L2TP...	SSL ...	Use ...	Allo...	Time...	Traffi...	Edit
☑	test	true	false	Disable	Disable	1440	Enable	Disable	Disable	Disable	Disable	0/-1	0/-1	✎

- ▶ Source User Group
- ▶ Source LDAP Group

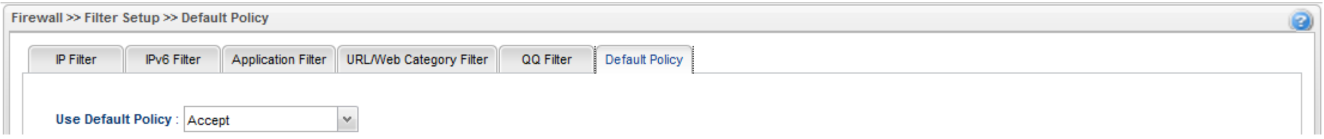
⊟ Destination IP

- ◢ Destination IP Object

□	Profile	Address Type	Start IP Address	End IP Address	Subnet Mask	Edit
☑	subnet_local	Subnet	192.168.0.0		255.255.255.0	✎
□	server_local	Single	192.168.0.10			✎

- ▶ Destination IP Group
- ▶ Destination DNS Object
- ▶ Destination User Profile
- ▶ Destination User Group
- ▶ Destination LDAP Group

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.


Firewall >> Filter Setup >> Default Policy

Use Default Policy : Accept

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