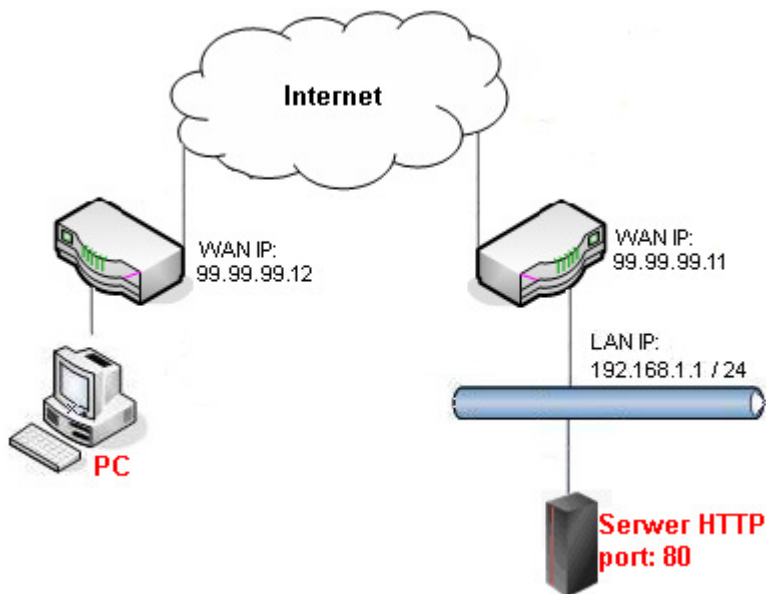


Metoda 1 – użycie jednej grupy IP Filter

Metoda 2 – użycie dwóch grup IP Filter



Główne założenia:

- Poprzez przekierowanie portu 80 do serwera HTTP ma dostęp tylko urządzenie prezentujące się adresem 99.99.99.12
- Publiczny adres IP zdalnego PC 99.99.99.12
- Prywatny adres IP serwera HTTP 192.168.1.6

Przejdź do zakładki **NAT>>Port Redirection**. Stwórz odpowiedni profil przekierowania portu.

NAT >> Port Redirection

Port Redirection

Add Edit Delete Refresh Move Up Move Down Rename Profile Number Limit : 256

Profile	Enable	WAN Profile	Use IP Alias	Alias	Private IP	Protocol	Port Redire...	Public Port ...	Public Port ...	Private Port
1	HTTP	true	wan1	No	192.168.1.6	TCP	One-to-One	80	80	80

Port Redirection

Profile : HTTP

Enable

WAN Profile : wan1

Use IP Alias : No

Private IP : 192 . 168 . 1 . 6


Protocol : TCP

Port Redirection Mode : One-to-One

Public Port : 80

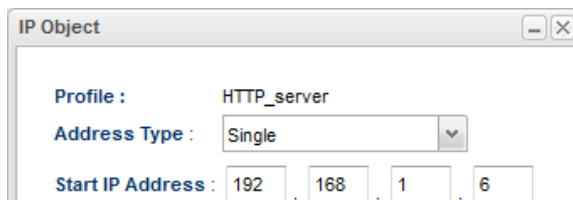
Private Port : 80

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

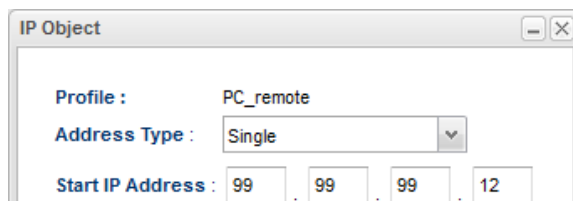


The screenshot shows a window titled "Objects Setting >> IP Object". Inside, there is a table with columns: Profile, Address Type, Start IP Address, End IP Address, and Subnet Mask. The table contains two entries: 1. HTTP\_server, Single, 192.168.1.6; 2. PC\_remote, Single, 99.99.99.12. Above the table are buttons for Add, Edit, Delete, and Refresh. A "Profile Number Limit : 200" indicator is visible in the top right corner of the table area.

	Profile	Address Type	Start IP Address	End IP Address	Subnet Mask
1	HTTP_server	Single	192.168.1.6		
2	PC_remote	Single	99.99.99.12		



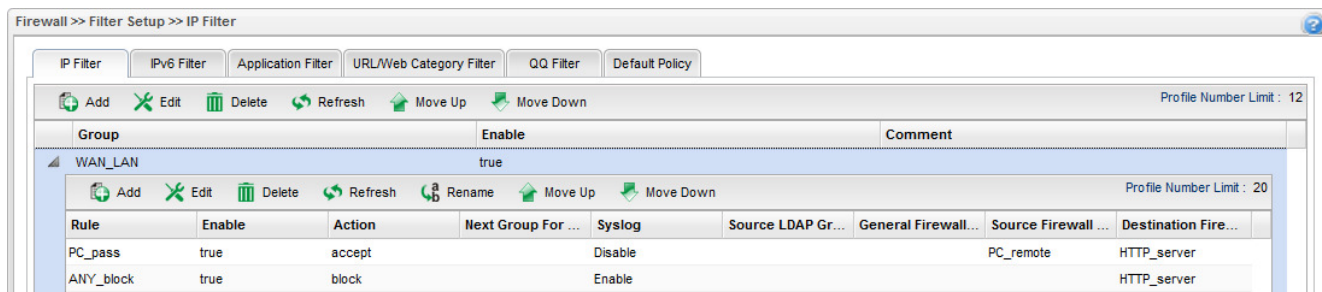
The dialog box is titled "IP Object". It contains the following fields:  
Profile : HTTP\_server  
Address Type : Single (dropdown menu)  
Start IP Address : 192 . 168 . 1 . 6 (four input boxes separated by dots)



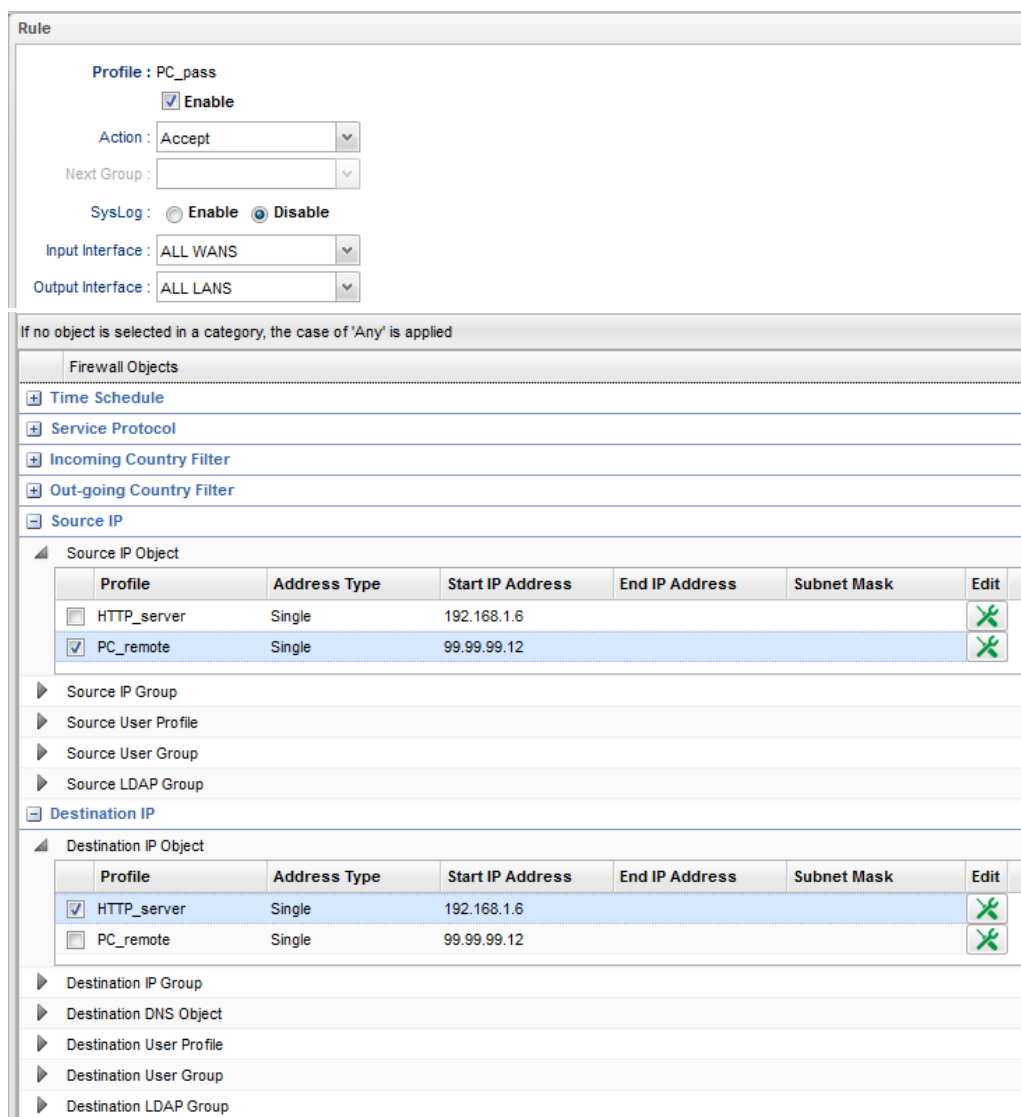
The dialog box is titled "IP Object". It contains the following fields:  
Profile : PC\_remote  
Address Type : Single (dropdown menu)  
Start IP Address : 99 . 99 . 99 . 12 (four input boxes separated by dots)

### Metoda 1 – użycie jednej grupy IP Filter

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



Reguła 'PC\_pass' – przepuszczanie ruchu od zdalnego PC do serwera HTTP



Reguła 'ANY\_block' – blokowanie ruchu od dowolnego urządzenia do serwera HTTP

Rule

Profile : ANY\_block

Enable

Action : Block

Next Group :

SysLog :  Enable  Disable

Input Interface : ALL WANS

Output Interface : ALL LANS

If no object is selected in a category, the case of 'Any' is applied

Firewall Objects

- Time Schedule
- Service Protocol
- Incoming Country Filter
- Out-going Country Filter
- Source IP
- Destination IP
  - Destination IP Object
 

Profile	Address Type	Start IP Address	End IP Address	Subnet Mask	Edit
<input checked="" type="checkbox"/> HTTP_server	Single	192.168.1.6			<input checked="" type="checkbox"/>
<input type="checkbox"/> PC_remote	Single	99.99.99.12			<input checked="" type="checkbox"/>
  - 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.

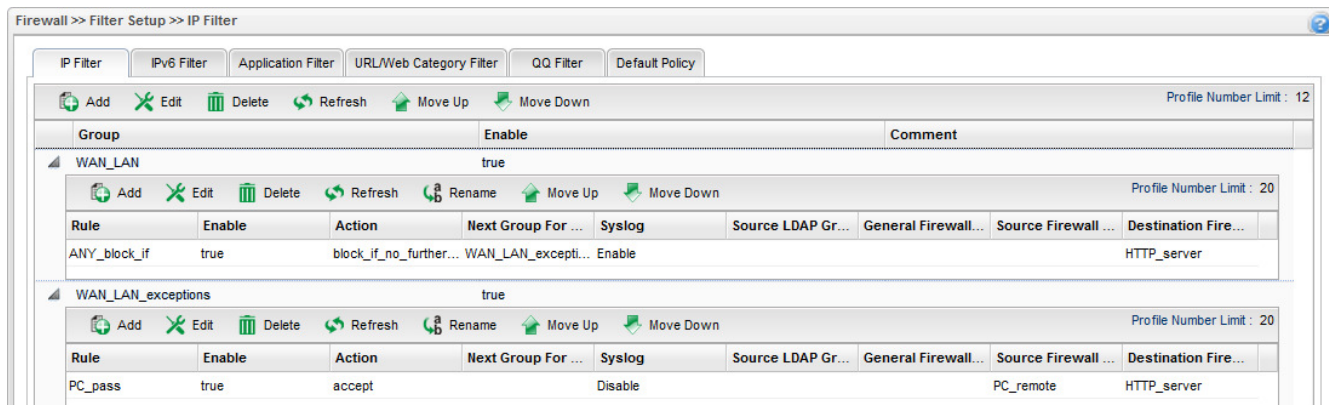
Firewall >> Filter Setup >> Default Policy

IP Filter IPv6 Filter Application Filter URL/Web Category Filter QQ Filter Default Policy

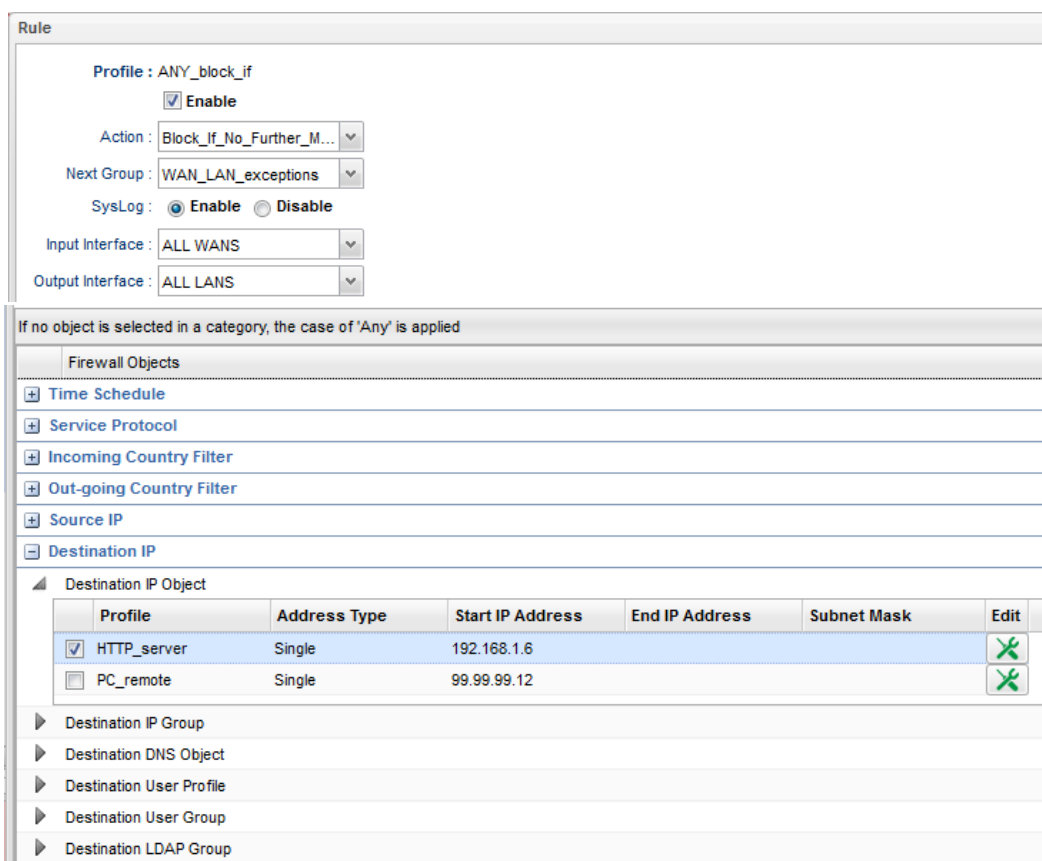
Use Default Policy : Accept

### Metoda 2 – użycie dwóch grup IP Filter

Przejdź do zakładki **Firewall>>Filter Setup>>IP Filter**. Stwórz odpowiednie grupy oraz reguły wybierając wcześniej stworzone profile obiektów.



Grupa 'WAN\_LAN' reguła 'ANY\_block\_if' – blokowanie całego ruchu z WAN do LAN od dowolnego urządzenia do serwera HTTP z weryfikacją reguł następnej grupy.



Grupa 'WAN\_LAN\_exceptions' reguła 'PC\_pass' – przepuszczanie ruchu od zdalnego PC do serwera HTTP

**Rule**

Profile : PC\_pass

Enable

Action : Accept

Next Group :

SysLog :  Enable  Disable

Input Interface : ALL WANS

Output Interface : ALL LANS

---

If no object is selected in a category, the case of 'Any' is applied

Firewall Objects

- Time Schedule
- Service Protocol
- Incoming Country Filter
- Out-going Country Filter
- Source IP
  - Source IP Object

Profile	Address Type	Start IP Address	End IP Address	Subnet Mask	Edit
<input type="checkbox"/> HTTP_server	Single	192.168.1.6			✕
<input checked="" type="checkbox"/> PC_remote	Single	99.99.99.12			✕

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

Profile	Address Type	Start IP Address	End IP Address	Subnet Mask	Edit
<input checked="" type="checkbox"/> HTTP_server	Single	192.168.1.6			✕
<input type="checkbox"/> PC_remote	Single	99.99.99.12			✕

  - 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

IP Filter   IPv6 Filter   Application Filter   URL/Web Category Filter   QQ Filter   **Default Policy**

Use Default Policy : Accept

Krzysztof Skowina  
 Specjalista ds. rozwiązań sieciowych  
 BRINET Sp. z o.o.  
[k.skowina@brinet.pl](mailto:k.skowina@brinet.pl)