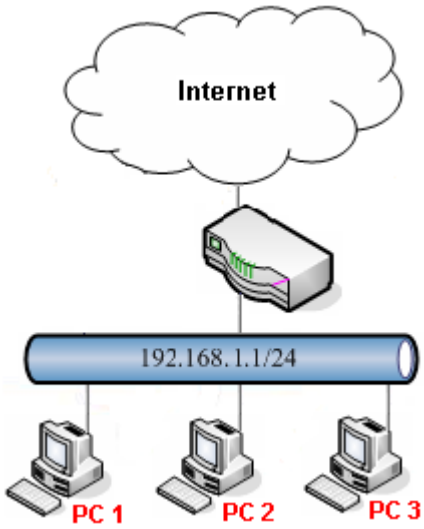
Metoda 1 – użycie jednej grupy IP Filter oraz Default Policy(Accept)
Metoda 2 – użycie jednej grupy IP Filter oraz Default Policy(Block)
Metoda 3 – użycie dwóch grup IP Filter

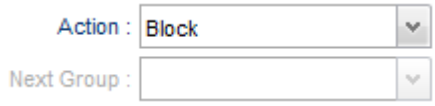


Główne założenia:

- PC1 (192.168.1.11) ma dostęp tylko do usług DNS(TCP/UDP 53), HTTP(TCP 80), HTTPS(TCP 443) z sieci LAN przez dowolny WAN (pozostałe usługi są blokowane).
- PC2 (192.168.1.12) oraz PC3 (192.168.1.13) nie mają ograniczeń.

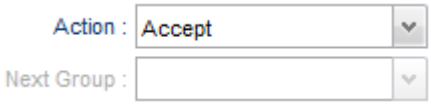
Uwagi:

1. Reguła **IP Filter** akcja **Block**:



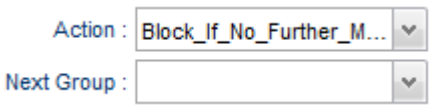
- ruch spełniający kryteria reguły IP Filter zostanie zablokowany natychmiast
- brak sprawdzania kolejnych reguł **IP Filter**, **Application Filter**, **URL/Web Category Filter**, **Default Policy**

2. Reguła **IP Filter** akcja **Accept:**



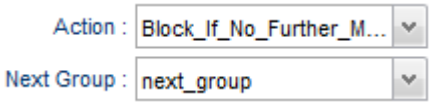
- ruch spełniający kryteria reguły IP Filter zostanie przepuszczony natychmiast
- brak sprawdzania kolejnych reguł **IP Filter**, **Application Filter**, **URL/Web Category Filter**, **Default Policy**

3. Reguła **IP Filter** akcja **Block_If_No_Further_Match** oraz nieokreślona następna grupa:



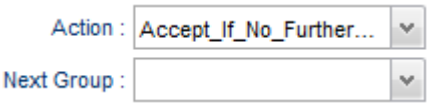
- ruch spełniający kryteria IP Filter zostanie zweryfikowany przez reguły **Application Filter**, **URL/Web Category Filter** i zostanie wykonana przypisana im akcja
- w przypadku braku pasujących reguł ruch zostanie zablokowany

4. Reguła **IP Filter** akcja **Block_If_No_Further_Match** oraz określona następna grupa:



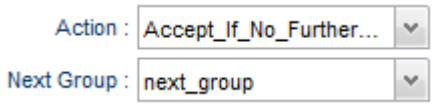
- ruch spełniający kryteria IP Filter zostanie zweryfikowany przez reguły **Next Group** i zostanie wykonana przypisana im akcja
- w przypadku braku pasujących reguł **Next Group** ruch zostanie zweryfikowany przez reguły **Application Filter**, **URL/Web Category Filter** i zostanie wykonana przypisana im akcja
- ostatecznie w przypadku braku pasujących reguł ruch zostanie zablokowany

5. Reguła **IP Filter** akcja **Accept_If_No_Further_Match** oraz nieokreślona następna grupa:



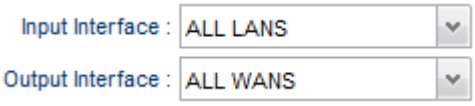
- ruch spełniający kryteria IP Filter zostanie zweryfikowany przez reguły **Application Filter**, **URL/Web Category Filter** i zostanie wykonana przypisana im akcja
- w przypadku braku pasujących reguł ruch zostanie przepuszczony

6. Reguła **IP Filter** akcja **Accept_If_No_Further_Match** oraz określona następna grupa:



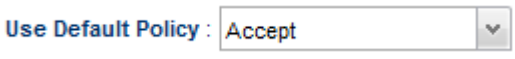
- ruch spełniający kryteria IP Filter zostanie zweryfikowany przez reguły **Next Group** i zostanie wykonana przypisana im akcja
- w przypadku braku pasujących reguł **Next Group** ruch zostanie zweryfikowany przez reguły **Application Filter**, **URL/Web Category Filter** i zostanie wykonana przypisana im akcja
- ostatecznie w przypadku braku pasujących reguł ruch zostanie przepuszczony

7. Reguła IP Filter dla ruchu z dowolnego LANu przez dowolny WAN:
- Input Interface: **ALL LANS**
- Output Interface: **ALL WANS**



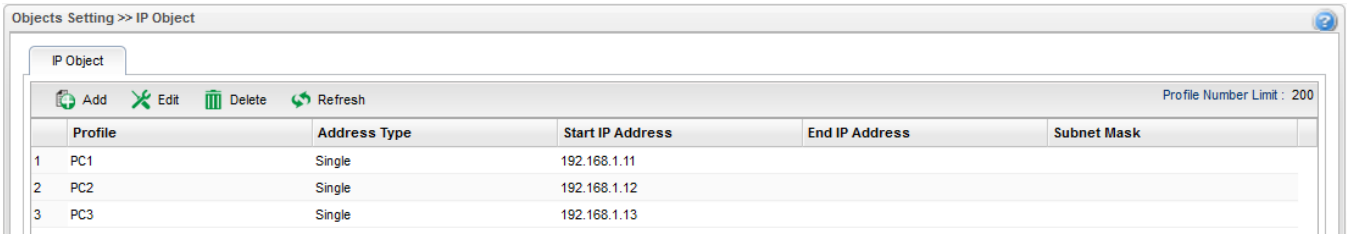
8. Proszę ostrożnie używać akcji **Block** dla Input/Output Interface **Any**

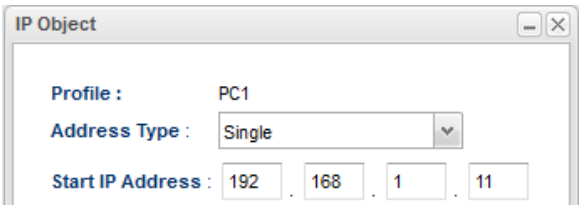
9. Default Policy:

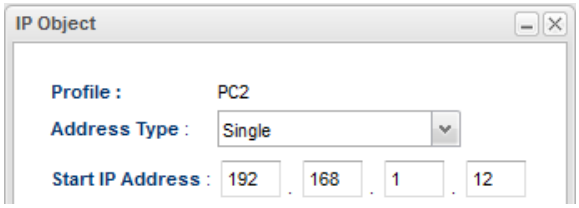


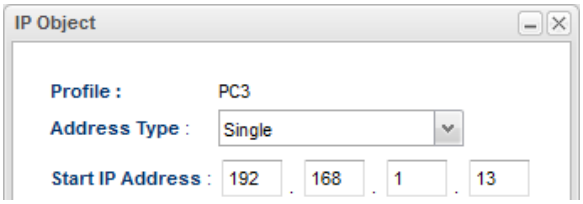
- dotyczy ruchu z dowolnego LANu przez dowolny WAN
- akcja **Block**/**Accept** zostanie wykonana jeśli ruch nie spełnił kryteriów **IP Filter**, **Application Filter**, **URL/Web Category Filter**

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



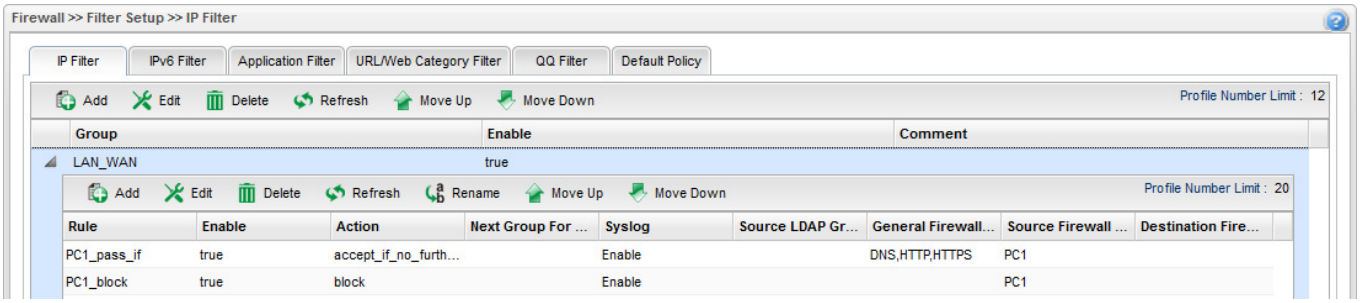




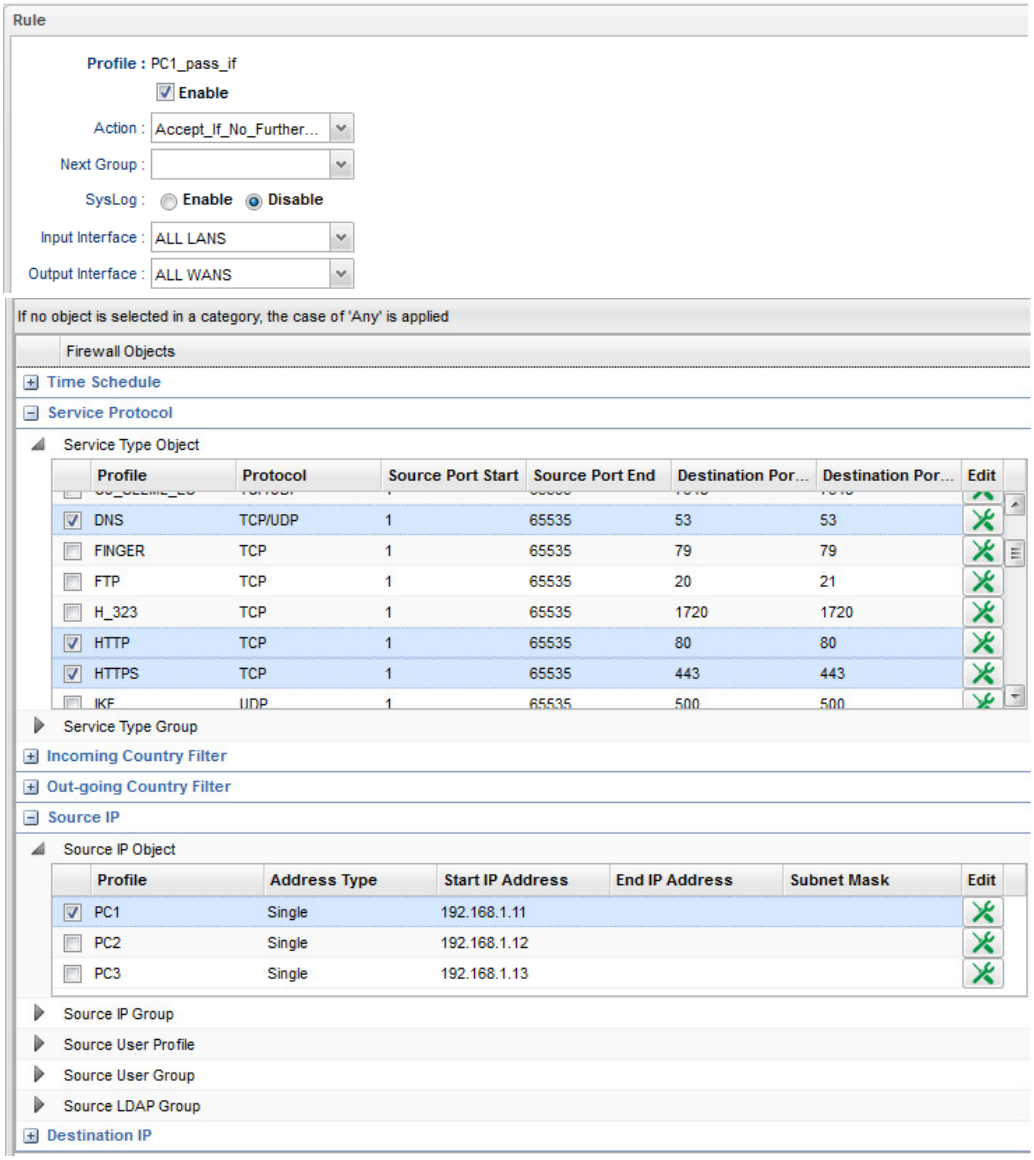


Metoda 1 – użycie jednej grupy IP Filter oraz Default Policy(Accept)

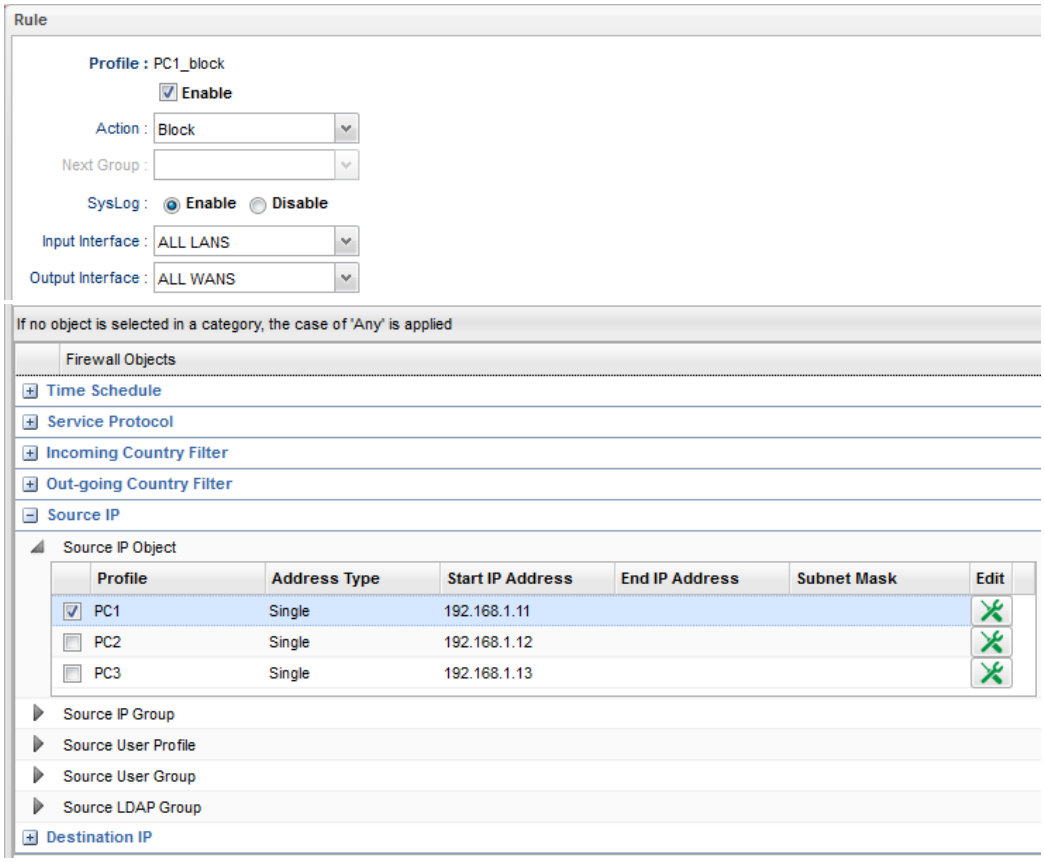
Przejdź do zakładki **Firewall>>Filter Setup>>IP Filter**. Stwórz odpowiednią grupę oraz reguły wybierając wcześniej stworzone profile obiektów.



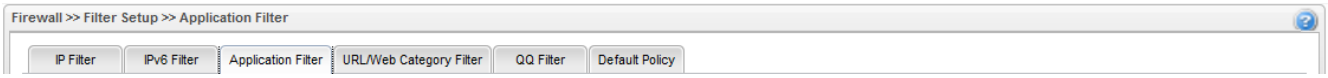
Reguła 'PC1_pass_if' – przepuszczanie ruchu DNS, HTTP, HTTPS od PC1 z weryfikacją reguł Application Filter, URL/Web Category Filter



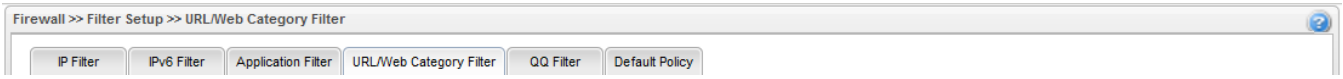
Reguła 'PC1_block' – blokowanie pozostałego ruchu od PC1



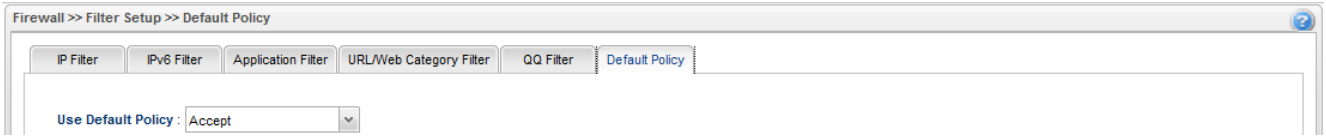
Przejdź do zakładki **Firewall>>Filter Setup>>Application Filter**. Jeśli dodałeś profile Filtru Aplikacji to upewnij się, że protokoły DNS, HTTP, HTTPS(SSL/TLS) nie są blokowane.



Przejdź do zakładki **Firewall>>Filter Setup>>URL/Web Category Filter**. Jeśli dodałeś profile Filtru URL/Kategorii Web to upewnij się, że ruch WWW do Internetu nie jest blokowany.

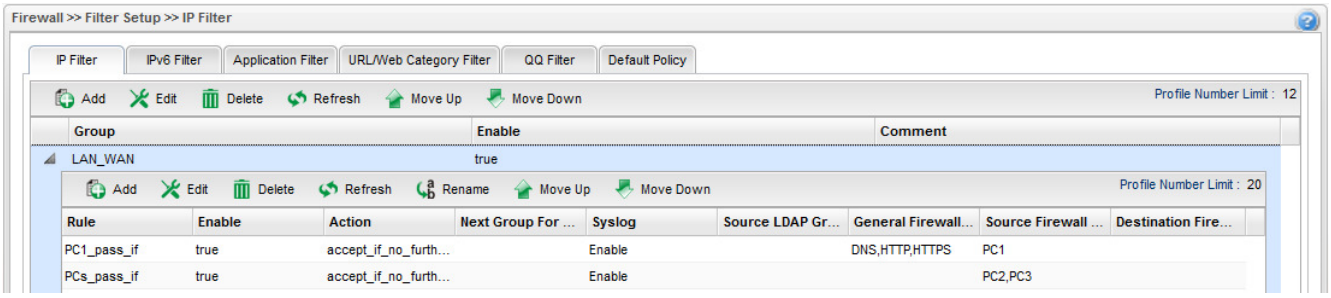


Przejdź do zakładki **Firewall>>Filter Setup>>Default Policy**. Domyślnie router przepuszcza ruch do Internetu, który nie spełnia kryteriów Filtru IP, Filtru Aplikacji, Filtru URL/Kategorii Web.
W celu przepuszczania pozostałego ruchu m.in. od PC2, PC3 wybierz **Accept**.

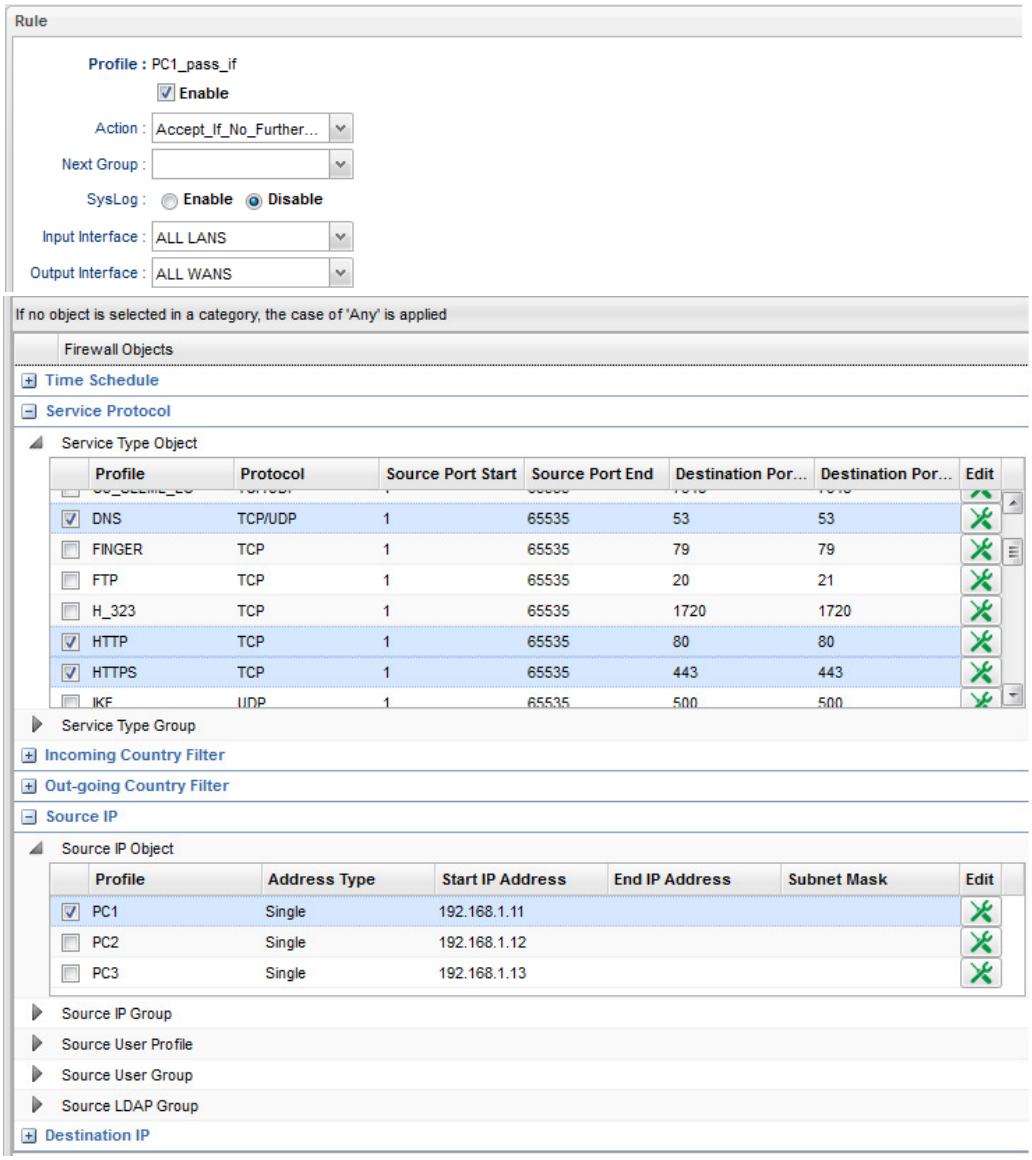


Metoda 2 – użycie jednej grupy IP Filter oraz Default Policy(Block)

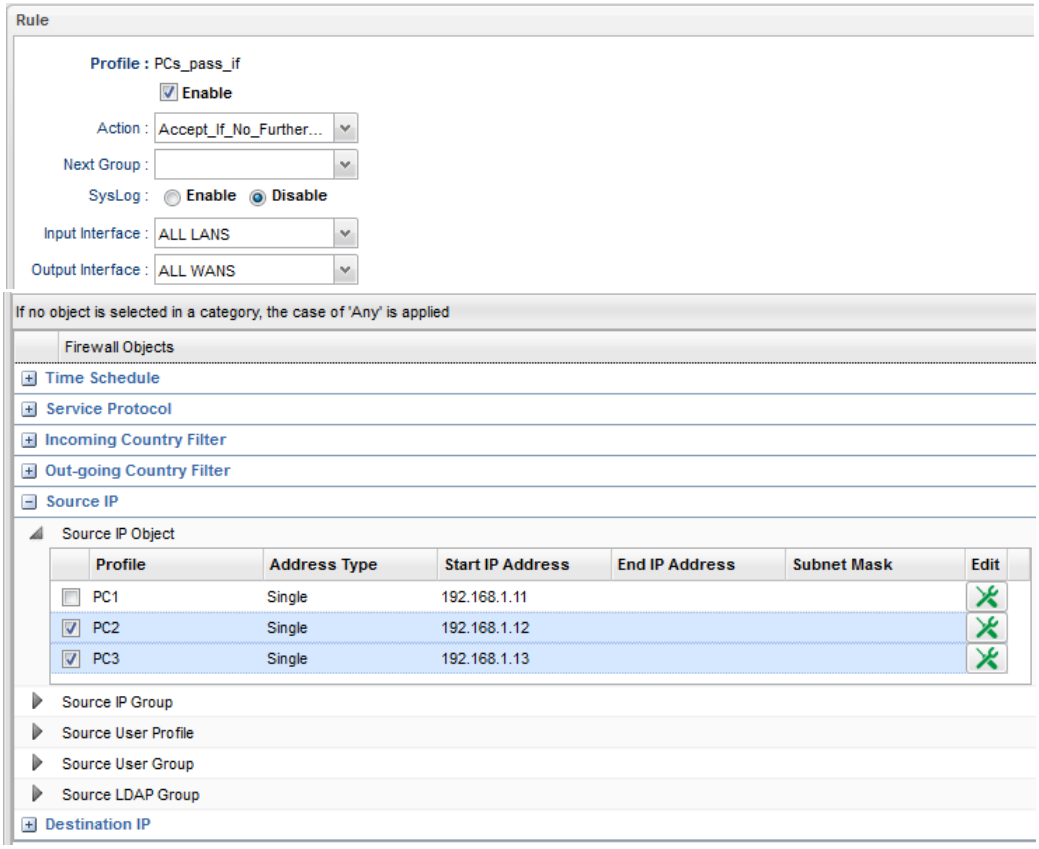
Przejdź do zakładki **Firewall>>Filter Setup>>IP Filter**. Stwórz odpowiednią grupę oraz reguły wybierając wcześniej stworzone profile obiektów.



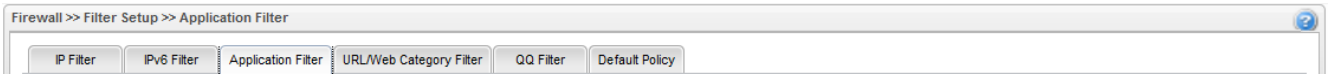
Reguła 'PC1_pass_if' – przepuszczanie ruchu DNS, HTTP, HTTPS od PC1 z weryfikacją reguł Application Filter, URL/Web Category Filter



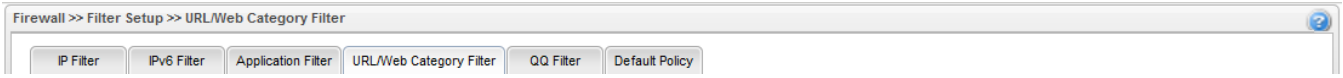
Reguła ‘PCs_pass_if’ – przepuszczanie całego ruchu od PC2 oraz PC3 z weryfikacją reguł Application Filter, URL/Web Category Filter



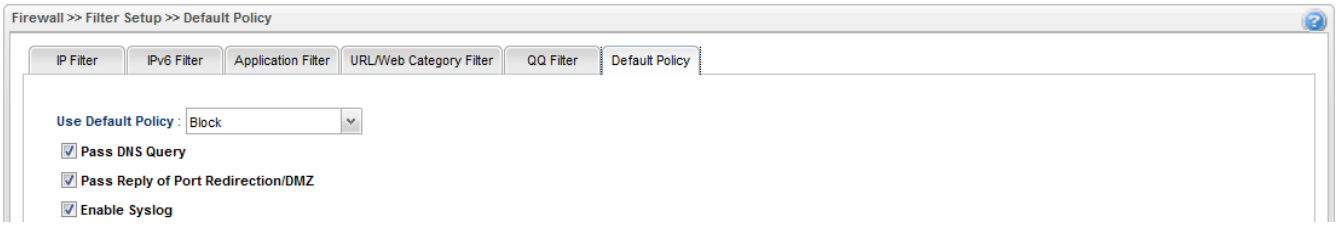
Przejdź do zakładki **Firewall>>Filter Setup>>Application Filter**. Jeśli dodałeś profile Filtru Aplikacji to upewnij się, że protokoły DNS, HTTP, HTTPS(SSL/TLS) nie są blokowane.



Przejdź do zakładki **Firewall>>Filter Setup>>URL/Web Category Filter**. Jeśli dodałeś profile Filtru URL/Kategorii Web to upewnij się, że ruch WWW do Internetu nie jest blokowany.

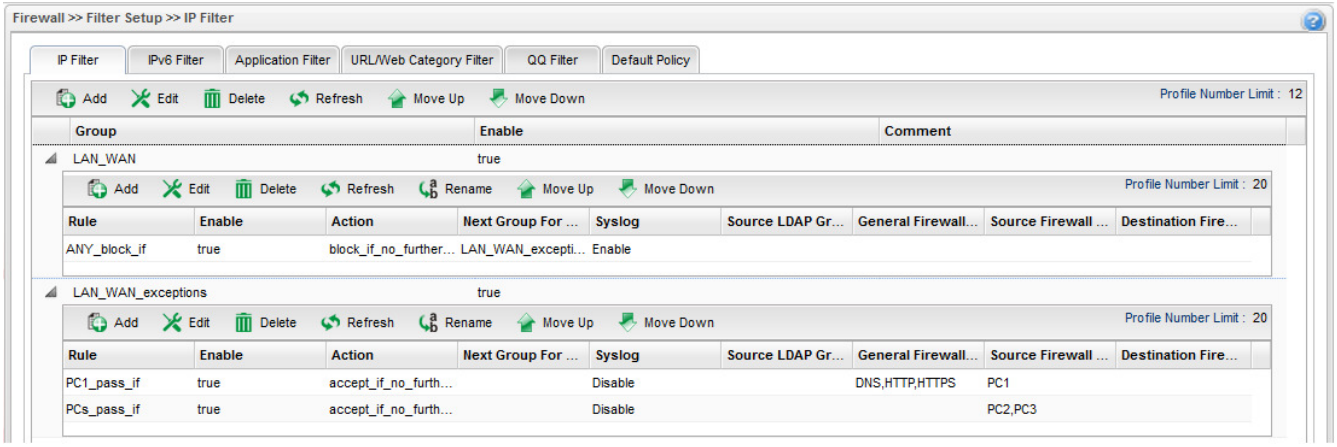


Przejdź do zakładki **Firewall>>Filter Setup>>Default Policy**. Domyślnie router przepuszcza ruch do Internetu, który nie spełnia kryteriów Filtru IP, Filtru Aplikacji, Filtru URL/Kategorii Web.
W celu blokowania pozostałego ruchu m.in. od PC1 wybierz **Block**.

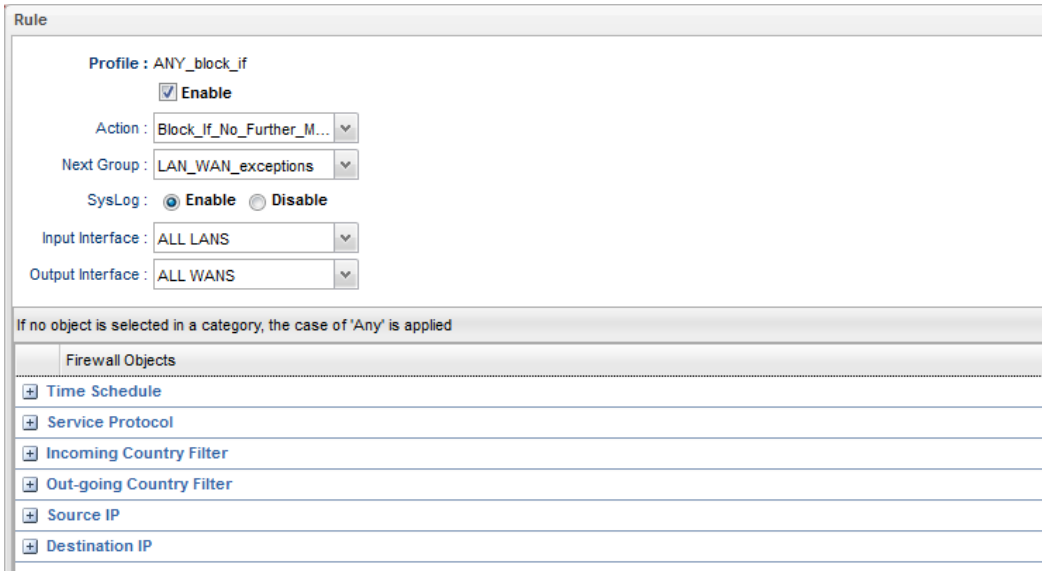


Metoda 3 – użycie dwóch grup IP Filter

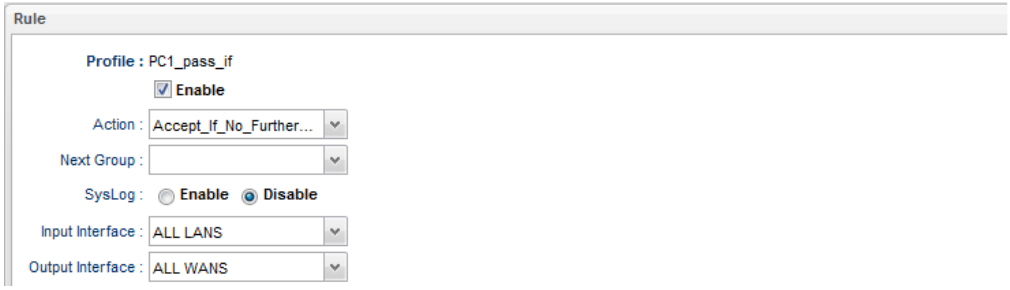
Przejdź do zakładki **Firewall>>Filter Setup>>IP Filter**. Stwórz odpowiednie grupy oraz reguły wybierając wcześniej stworzone profile obiektów.

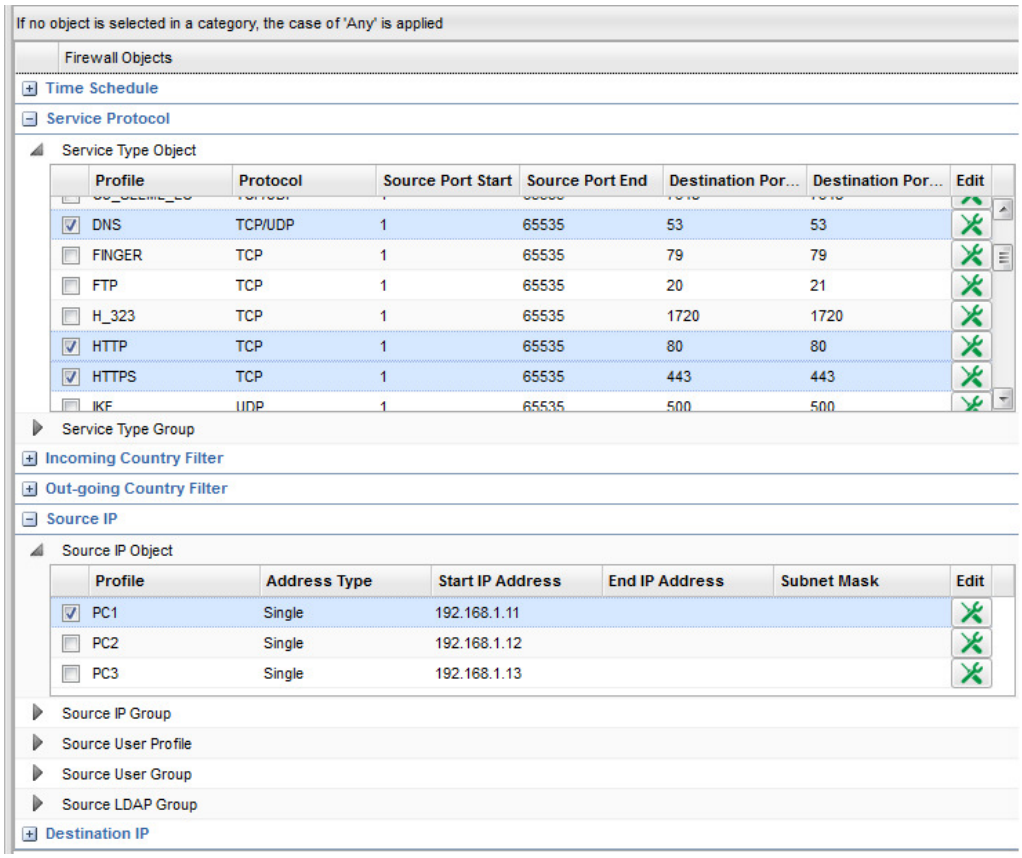


Grupa 'LAN_WAN' reguła 'ANY_block_if' – blokowanie całego ruchu z LAN do WAN od dowolnego urządzenia z weryfikacją reguł następnej grupy.

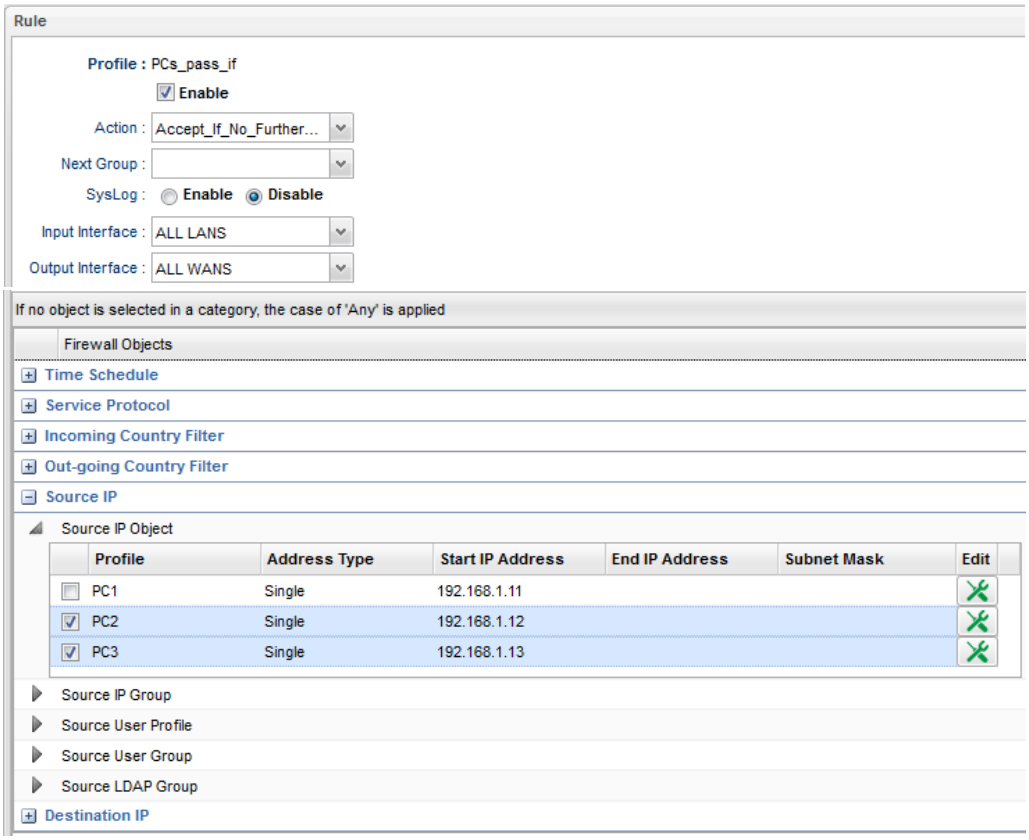


Grupa 'LAN_WAN_exceptions' reguła 'PC1_pass_if' – przepuszczanie ruchu DNS, HTTP, HTTPS od PC1 z weryfikacją reguł Application Filter, URL/Web Category Filter

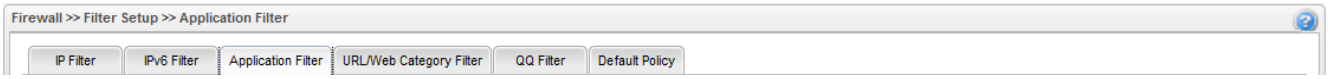




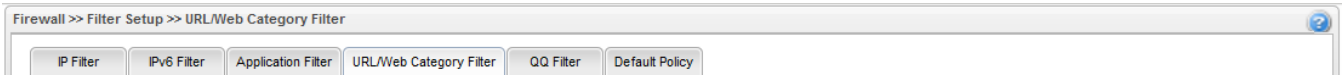
Grupa 'LAN_WAN_exceptions' reguła 'PCs_pass_if' – przepuszczanie całego ruchu od PC2 oraz PC3 z weryfikacją reguł Application Filter, URL/Web Category Filter



Przejdź do zakładki **Firewall>>Filter Setup>>Application Filter**. Jeśli dodałeś profile Filtru Aplikacji to upewnij się, że protokoły DNS, HTTP, HTTPS(SSL/TLS) nie są blokowane.



Przejdź do zakładki **Firewall>>Filter Setup>>URL/Web Category Filter**. Jeśli dodałeś profile Filtru URL/Kategorii Web to upewnij się, że ruch WWW do Internetu nie jest blokowany.



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