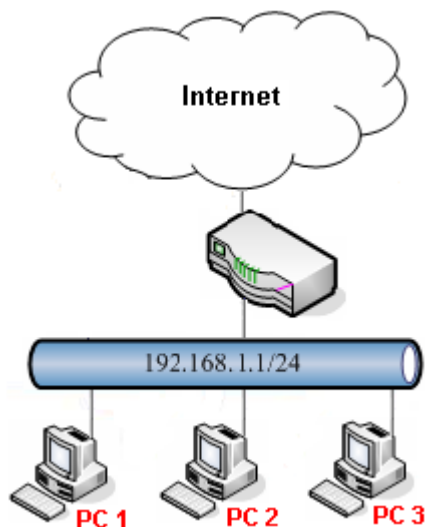


Metoda 1 – użycie jednej grupy IP Filter oraz Default Policy(Accept)

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:

Action :

Next Group :

- 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:

Action :

Next Group :

- 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:

Action :

Next Group :

- 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:

Action : ▼
 Next Group : ▼

- 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:

Action : ▼
 Next Group : ▼

- 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:

Action : ▼
 Next Group : ▼

- 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**

Input Interface : ▼
 Output Interface : ▼

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

Action : ▼
 Next Group : ▼
 Input Interface : ▼
 Output Interface : ▼

9. **Default Policy:**

Use 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.

Objects Setting >> IP Object

IP Object

Add Edit Delete Refresh Profile Number Limit : 200

Profile	Address Type	Start IP Address	End IP Address	Subnet Mask
1 PC1	Single	192.168.1.11		
2 PC2	Single	192.168.1.12		
3 PC3	Single	192.168.1.13		

IP Object

Profile : PC1

Address Type : Single

Start IP Address : 192 . 168 . 1 . 11

IP Object

Profile : PC2

Address Type : Single

Start IP Address : 192 . 168 . 1 . 12

IP Object

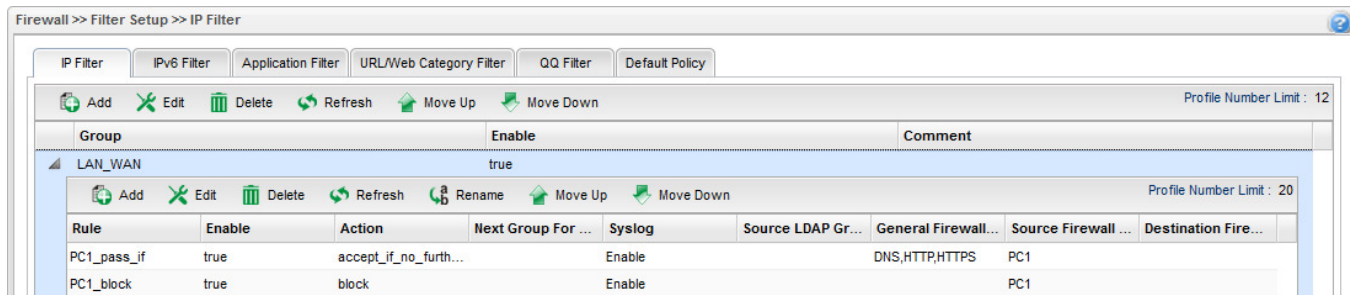
Profile : PC3

Address Type : Single

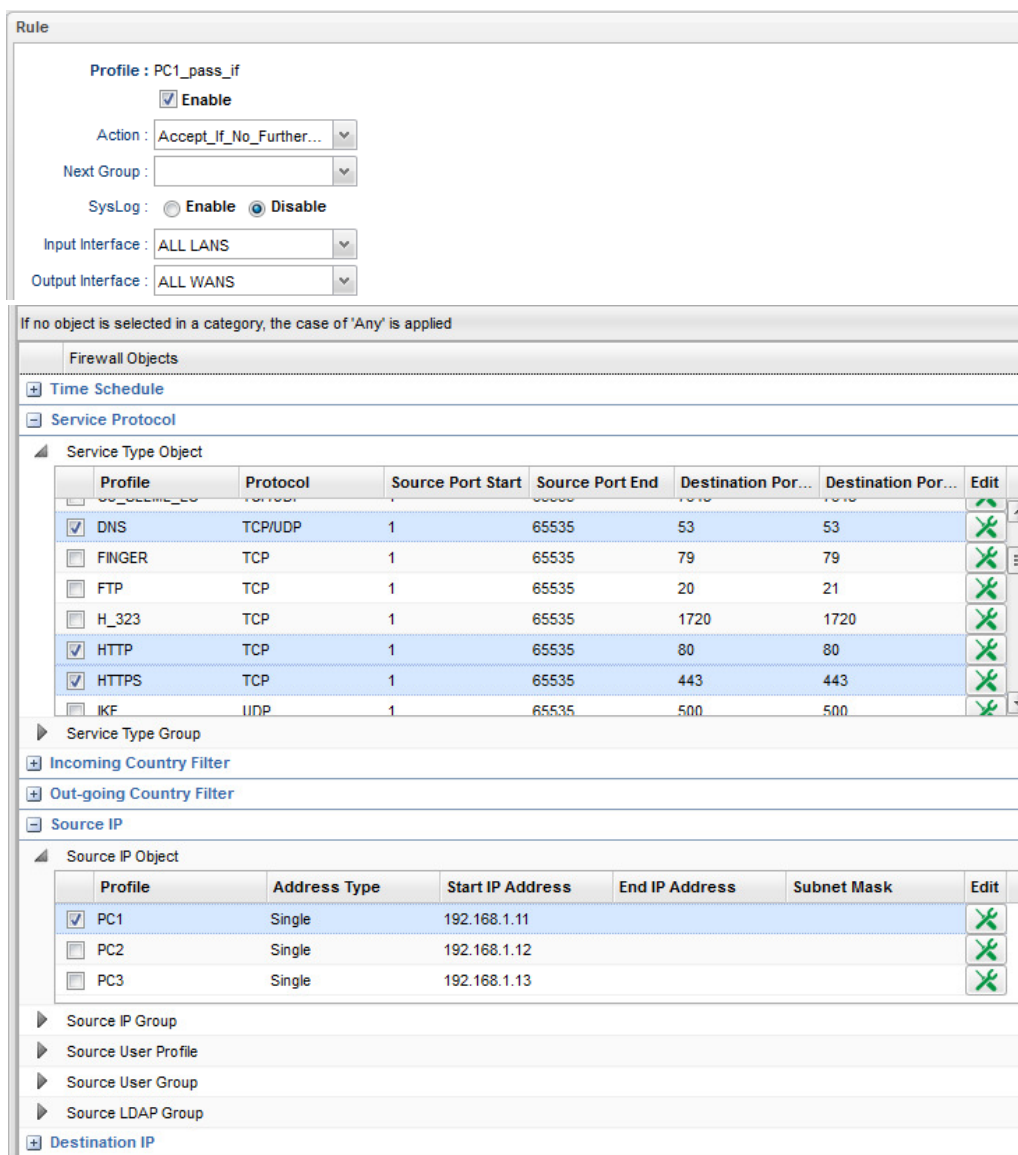
Start IP Address : 192 . 168 . 1 . 13

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

Rule

Profile : PC1_block

Enable

Action : Block

Next Group :

SysLog : Enable Disable

Input Interface : ALL LANS

Output Interface : ALL WANS

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 checked="" type="checkbox"/> PC1	Single	192.168.1.11			
<input type="checkbox"/> PC2	Single	192.168.1.12			
<input type="checkbox"/> PC3	Single	192.168.1.13			
 - Source IP Group
 - Source User Profile
 - Source User Group
 - Source LDAP Group
- Destination IP

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.

Firewall >> Filter Setup >> Application Filter

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

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.

Firewall >> Filter Setup >> URL/Web Category Filter

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

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**.

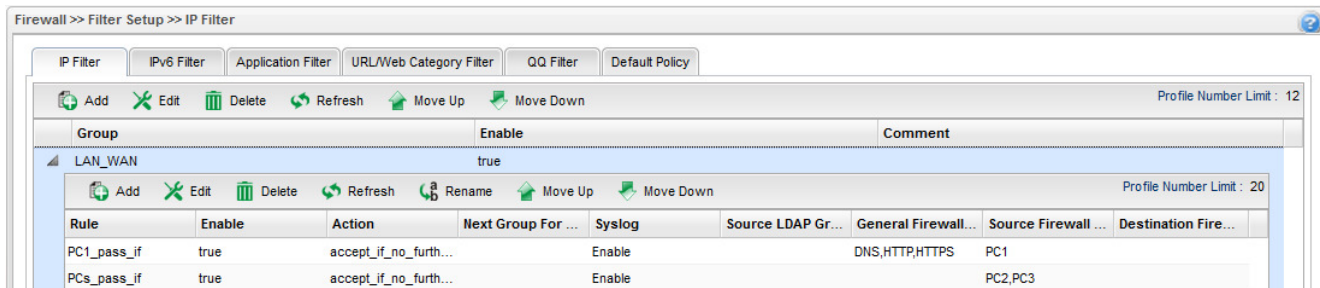
Firewall >> Filter Setup >> Default Policy

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

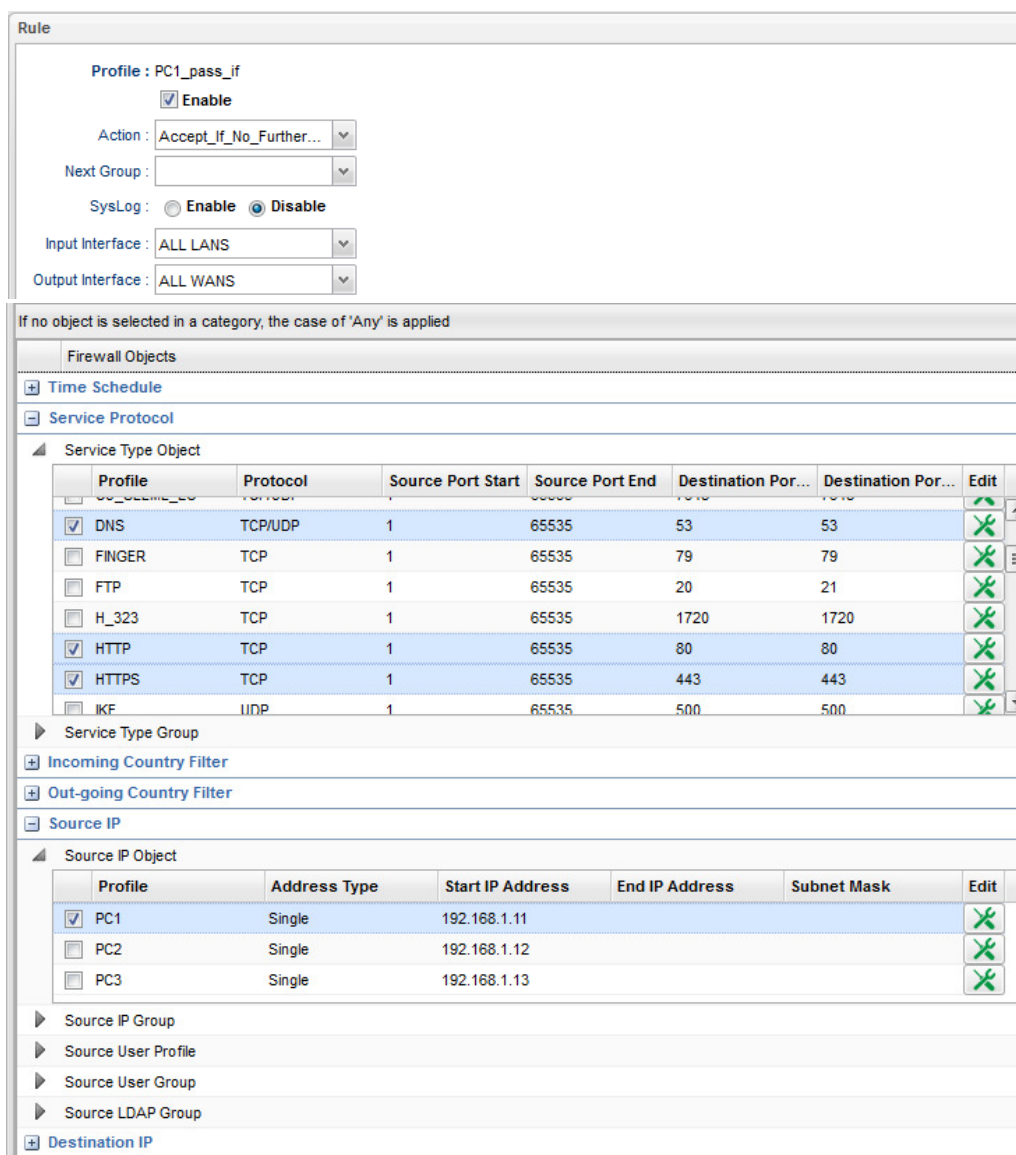
Use Default Policy : Accept

Metoda 2 – użycie 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

Rule

Profile : PCs_pass_if

Enable

Action : Accept_if_No_Further... ▾

Next Group : ▾

SysLog : Enable Disable

Input Interface : ALL LANS ▾

Output Interface : ALL WANS ▾

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"/> PC1	Single	192.168.1.11			
<input checked="" type="checkbox"/> PC2	Single	192.168.1.12			
<input checked="" type="checkbox"/> PC3	Single	192.168.1.13			
 - Source IP Group
 - Source User Profile
 - Source User Group
 - Source LDAP Group
- Destination IP

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.

Firewall >> Filter Setup >> Application Filter

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

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.

Firewall >> Filter Setup >> URL/Web Category Filter

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

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**.

Firewall >> Filter Setup >> Default Policy

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

Use Default Policy : Block ▾

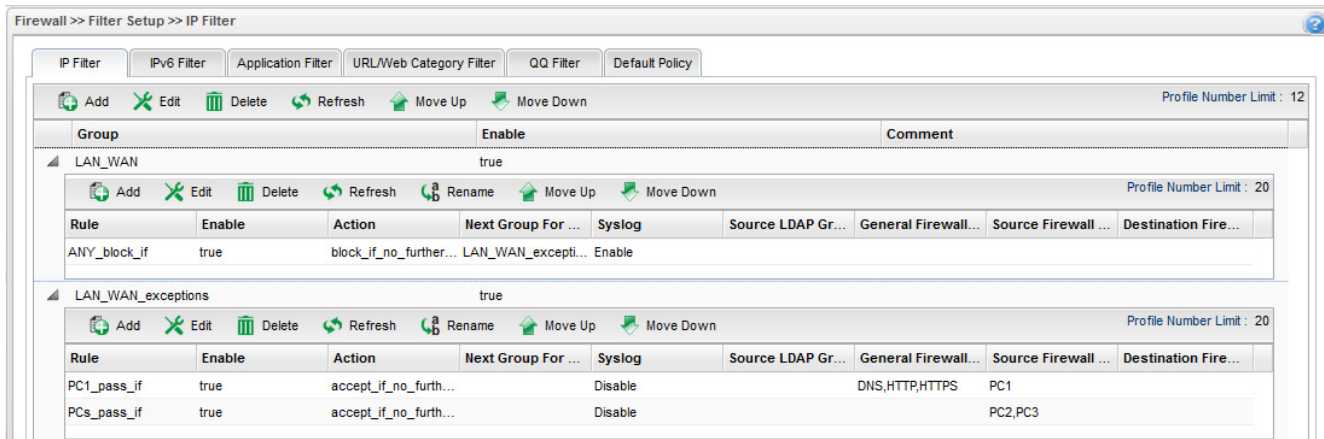
Pass DNS Query

Pass Reply of Port Redirection/DMZ

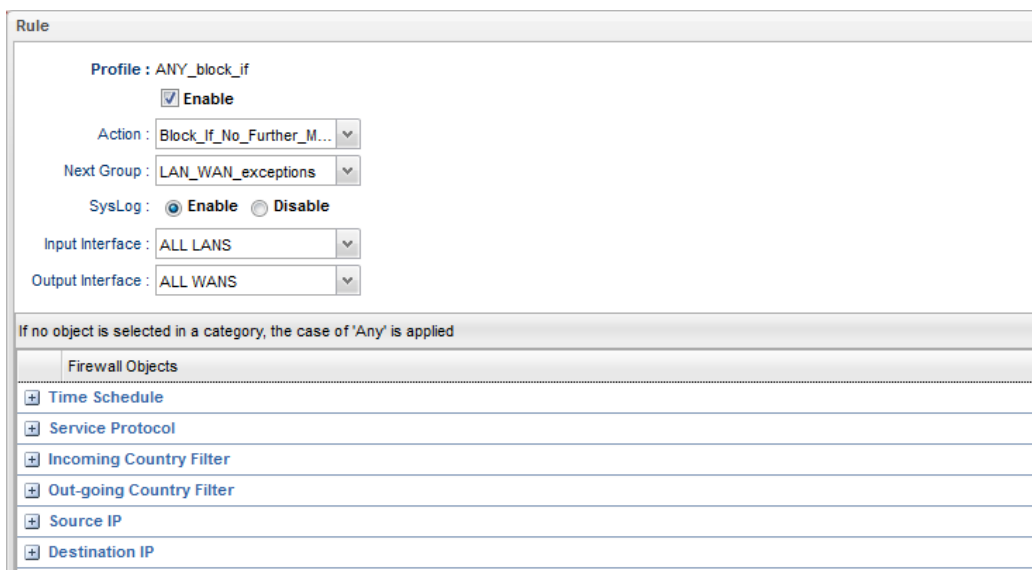
Enable Syslog

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



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

Firewall Objects

- Time Schedule
- Service Protocol
 - Service Type Object

Profile	Protocol	Source Port Start	Source Port End	Destination Port Start	Destination Port End	Edit
<input checked="" type="checkbox"/> DNS	TCP/UDP	1	65535	53	53	
<input type="checkbox"/> FINGER	TCP	1	65535	79	79	
<input type="checkbox"/> FTP	TCP	1	65535	20	21	
<input type="checkbox"/> H_323	TCP	1	65535	1720	1720	
<input checked="" type="checkbox"/> HTTP	TCP	1	65535	80	80	
<input checked="" type="checkbox"/> HTTPS	TCP	1	65535	443	443	
<input type="checkbox"/> IKF	IUDP	1	65535	500	500	
 - Service Type Group
 - 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 checked="" type="checkbox"/> PC1	Single	192.168.1.11			
<input type="checkbox"/> PC2	Single	192.168.1.12			
<input type="checkbox"/> PC3	Single	192.168.1.13			
 - Source IP Group
 - Source User Profile
 - Source User Group
 - Source LDAP Group
 - Destination IP

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

Rule

Profile : PCs_pass_if

Enable

Action : Accept_if_No_Further...

Next Group :

SysLog : Enable Disable

Input Interface : ALL LANS

Output Interface : ALL WANS

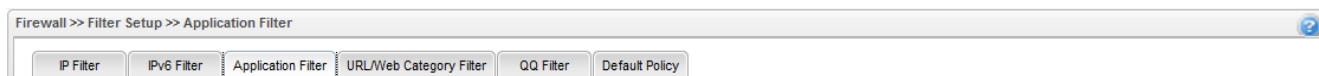
If no object is selected in a category, the case of 'Any' is applied

Firewall Objects

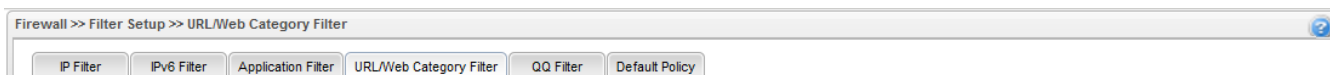
- Time Schedule
- Service Protocol
- Incoming Country Filter
- Out-going Country Filter
- Source IP
 - Source IP Object

Profile	Address Type	Start IP Address	End IP Address	Subnet Mask	Edit
<input type="checkbox"/> PC1	Single	192.168.1.11			
<input checked="" type="checkbox"/> PC2	Single	192.168.1.12			
<input checked="" type="checkbox"/> PC3	Single	192.168.1.13			
 - Source IP Group
 - Source User Profile
 - Source User Group
 - Source LDAP Group
- Destination IP

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