

- 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 :	Block	۷
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 :	Accept	۷
Next Group :		Y

- 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 :	Block_If_No_Further_M	۷	
Next Group :		٧	

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 : Block_If_No_Further_M	×
--------------------------------	---

Next Group : 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 :	Accept_If_No_Further	۷
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 :	Accept_If_No_Further	۷
Next Group :	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 :	ALL LANS	۷
Output Interface :	ALL WANS	۷

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

Action :	Block	*
Next Group :		×
Input Interface :	Any	~
Output Interface :	Any	~

#### 9. Default Policy:

Use Default Policy : Accept

- 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.

Ot	jects	s Setting >> IP Object				2
Ι,	IF	P Object				
	1	🚯 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	
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.

IP Filter IPv	6 Filter Application Filter	URL/Web Categor	y Filter QQ Filter	Default Policy				
🚯 Add 🛛 🗶 E	dit 👖 Delete 🛭 📢 Re	fresh 🛛 👉 Move U	ip 😽 Move Down					Profile Number Limi
Group			Enable			Comment		
LAN_WAN			true					
🚺 Add	🗶 Edit 👖 Delete 🗳	Refresh Ga Re	ename 🛛 👉 Move U	p 🛛 🐣 Move Dow	'n			Profile Number Limit: 20
Rule	Enable	Action	Next Group For	Syslog	Source LDAP Gr	General Firewall	Source Firewall	Destination Fire
700000		accept if an furth		Enable		DNS HTTP HTTPS	PC1	
PC1_pass_if	true	iccept_ii_iio_iuriii		Chable		bilo,initi,initi o	101	

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

lule								
	Profile : PC	1_pass_if						
		Enable						
	Action : A	ccept_If_No_Further 👻						
	Next Group :	~						
	SysLog : (	Enable () Disable						
In	out Interface : A							
Out								
Out	A A A A A A A A A A A A A A A A A A A							_
lf no d	bject is selected	in a category, the case of '	Any' is applied					
	Firewall Object	S						
+ T	ime Schedule							_
- s	ervice Protoco							_
4	Service Type O	bject	Course Doublet	Course Doub Ford	Destination Des	De etie etie e De e	F-04	_
-	Profile	Protocol	Source Port Start	Source Port End	Destination Por	Destination Por	Edit	
	DNS	TCP/UDP	1	65535	53	53	×	-
	FINGER	тср	1	65535	79	79	×	H
	FTP	TCP	1	65535	20	21	×	
	H_323	TCP	1	65535	1720	1720	×	
	V HTTP	TCP	1	65535	80	80	×	
	HTTPS	TCP	1	65535	443	443	×	
	IKF	UDP	1	65535	500	500	X	-
•	Service Type G	roup						
	ncoming Count	ry Filter						_
± 0	our-going Coun	try Filter						_
	Source IP Obios							_
-	Drofile	Address T	vne Start ID Ad	drace End ID	Address Su	hnet Maek	Edit	-
		Single	102 168 1 1		Address Su	Difet mask	Lun	_
	PC2	Single	192 168 1 1	2			÷	
	PC3	Single	192.168.1.1	3			Ŷ	
h		1						_
P	Source IP Group	p er						
P	Source User Pr	ofile						
P b	Source User Gr	oup						
	Source LDAP G	oup						



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 select	ted in a category	the case of 'Any	is applied			
Firewall Ohi	acte	, the case of Any				
Time Schedu						
Service Proto						
	untry Filter					
Incoming Cot	untry Filtor					
Course IP	unity ritter					
	vicet					
A Source P OL	neci	Address Trees	Ctart ID A datases		Cube of March	E-114
Profile		Address Type	Start IP Address	Ella IP Address	Subnet Mask	Euit
PC1		Single	192.168.1.11			X
PC2		Single	192.168.1.12			×
PC3		Single	192.168.1.13			×
Source IP Gr	oup					
Source User	Profile					
Source User	Group					
Source LDA	P Group					
Destination IF						

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.

Fin	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**.

Fin	wall >> Filter \$	Setup >> Defau	It Policy			0
	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.

IP Filter IPv	6 Filter Application Fil	ter URL/Web Categor	y Filter QQ Filter	Default Policy				
🚯 Add 🛛 🗶 Ed	dit <u> m</u> Delete 🔇 🍏	Refresh 🛛 👉 Move l	Jp 🛛 🐣 Move Down					Profile Number Limit
Group			Enable			Comment		
LAN_WAN			true					
🚯 Add 🔀 Edit 🏢 Delete 📣 Refresh 🖧 Rename 🍲 Move Up 😽 Move Down				Profile Number Limit: 20				
	Enable	Action	Next Group For	Syslog	Source LDAP Gr	General Firewall	Source Firewall	Destination Fire
Rule								
Rule PC1_pass_if	true	accept_if_no_furth		Enable		DNS,HTTP,HTTPS	PC1	

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

Rule								
	Profile : PC1_pa	ss_if						
	V Ena	ble						
	Action : Accept	_lf_No_Further 👻						
	Next Group :	*						
	SysLog : 🔘 Ena	able 💿 Disable						
In	put Interface : ALL LA	NS Y						
0	put Interface : ALL W							
	ALL W	ANG T						_
If no (	object is selected in a c	category, the case of 'A	kny' is applied					_
	Firewall Objects							
± 1	ime Schedule							_
<u> </u>	ervice Protocol							_
4	Service Type Object							_
	Profile	Protocol	Source Port Start	Source Port End	Destination Por	Destination Por	Edit	
	DNS	TCP/UDP	1	65535	53	53	×	
	FINGER	TCP	1	65535	79	79	×	
	FTP	TCP	1	65535	20	21	×	Γ
	H_323	TCP	1	65535	1720	1720	×	
	✓ HTTP	TCP	1	65535	80	80	×	
	HTTPS	тср	1	65535	443	443	×	L
	IKF	UDP	1	65535	500	500	X	-
	Service Type Group							
+ I	ncoming Country Fil	ter						_
+ 0	out-going Country Fi	lter						
- s	ource IP							_
4	Source IP Object						1	_
	Profile	Address Ty	pe Start IP Ad	Idress End IP	Address Su	bnet Mask	Edit	
	PC1	Single	192.168.1.1	1			×	
	PC2	Single	192.168.1.1	2			×	
	PC3	Single	192.168.1.1	3			×	
▶	Source IP Group							
₽	Source User Profile							
₽	Source User Group							
▶	Source LDAP Group							
+ 0	estination IP							

7/10



Reguła 'PCs\_pass\_if' – przepuszczanie całego ruchu od PC2 oraz PC3 z weryfikacją reguł Application Filter, URL/Web Category Filter

Rule						
Profil	e : PCs_pass_if					
	Enable					
Actio	n : Accept_If_No	_Further 🔻				
Next Grou	p :	~				
SysLo	g: 💿 Enable	Disable				
Input Interfac	e : ALL LANS	~				
Output Interfac		~				
f no object is sel	ected in a categor	y, the case of 'Any' is	applied			
Firewall O	bjects					
+ Time Scheo	lule					
<ul> <li>Service Pro</li> </ul>	tocol					
Incoming C	ountry Filter					
🛨 Out-going C	ountry Filter					
Source IP						
▲ Source IP	Object					
Profi	le	Address Type	Start IP Address	End IP Address	Subnet Mask	Edit
PC1		Single	192.168.1.11			×
PC2		Single	192.168.1.12			×
PC3		Single	192.168.1.13			×
Source IP	Group					
Source Us	er Profile					
Source Us	er Group					
Source LD	AP 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	irewall >> 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						Fi	
oolicy	Default Policy	QQ Filter	URL/Web Category Filter	Application Filter	IPv6 Filter	IP Filter	
olicy	Default Policy	QQ Filter	URL/Web Category Filter	Application Filter	IPv6 Filter	IP Filter	

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**.

ewall >> Filter Setup >> Default Policy						
IP Filter IPv6 Filter Application Filter URL/Web Category Filter QQ Filter Default Pol						
lise Default Policy Block y						
Use Default Policy : Block ▼ Pass DNS Query						
V 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.

IP	Filter IPv6	Filter Application F	ilter URL/Web Category	y Filter QQ Filter	Default Policy				
R	👌 Add 🛛 🔀 Ed	it <u> î</u> Delete 🧳	Refresh 🍲 Move U	p 🛛 🐣 Move Down					Profile Number Limi
	Group			Enable			Comment		
LAN_WAN true									
	🚺 Add 💙	🕻 Edit 🛛 🕅 Delete	🖨 Refresh 🖓 🖓 Re	ename 🛛 👉 Move U	p 🛛 🐣 Move Do	wn			Profile Number Limit: 20
F	Rule	Enable	Action	Next Group For	Syslog	Source LDAP Gr	General Firewall	Source Firewall	Destination Fire
	ANY_block_if	true	block_if_no_further	LAN_WAN_excepti	Enable				
	LAN_WAN_exce	ptions		true					
	🚯 Add 💙	🕻 Edit 🛛 🕅 Delete	Ϛ Refresh 🖓 🔓 Re	ename 🛛 👉 Move U	p 🛛 🐣 Move Do	wn			Profile Number Limit: 20
	Rule	Enable	Action	Next Group For	Syslog	Source LDAP Gr	General Firewall	Source Firewall	Destination Fire
1	PC1_pass_if	true	accept_if_no_furth		Disable		DNS,HTTP,HTTPS	PC1	
	PCs nass if	true	accept if no furth		Disable			PC2 PC3	

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

Rule	
Profile :	ANY_block_if
	C Enable
Action :	Block_If_No_Further_M Y
Next Group :	LAN_WAN_exceptions Y
SysLog :	Enable      Disable     Disable
Input Interface :	ALL LANS
Output Interface :	ALL WANS
Manager and the sector	
If no object is selec	ted in a category, the case of Any is applied
Firewall Obj	ects
Time Cebedu	
H Time schedu	
Service Prote	
Service Proto     Incoming Con	ie col intry Filter
Inne schedu     Service Proto     Incoming Con     Out-going Co	ie col untry Filter untry Filter
Time schedu     Service Proto     Incoming Com     Out-going Com     Source IP	ie bool untry Filter untry Filter

Grupa `LAN\_WAN\_exceptions' reguła `PC1\_pass\_if' – przepuszczanie ruchu DNS, HTTP, HTTPS od PC1 z weryfikacją reguł Application Filter, URL/Web Category Filter

Rule					
Profile : PC1_pass_if					
	Chable				
Action :	Accept_If_No_Further V				
Next Group :	~				
SysLog :	💿 Enable 💿 Disable				
Input Interface :	ALL LANS Y				
Output Interface :	ALL WANS 🗸				



	Fire	ewall Objects							
1	Time	Schedule							
	Servi	ce Protocol							
4	Ser	vice Type Object							
		Profile	Protocol	Source Port Start	Source Port End	Destination Por	Destination Por	Edit	
		00_000000_00	TOITODI		00000	1010	1010	~	
	V	DNS	TCP/UDP	1	65535	53	53	×	F
		FINGER	TCP	1	65535	79	79	×	
		FTP	TCP	1	65535	20	21	×	
		H_323	TCP	1	65535	1720	1720	×	1
	V	HTTP	TCP	1	65535	80	80	×	1
		HTTPS	тср	1	65535	443	443	×	1
		IKF	UDP	1	65535	500	500	X	E
	S	in a Country Filt							
	Dut-g Sourc	joing Country Filt ce IP	er						
	Dut-g Sourc Sou	joing Country Filt ce IP urce IP Object	er						
	Dut-g Sourc Sou	ooing Country Filt ce IP urce IP Object Profile	Address T	ype Start IP Ad	dress End IP	Address Su	bnet Mask	Edit	:
4	Source Source Source	ooing Country Filt ce IP urce IP Object Profile PC1	er Address T Single	ype Start IP Ad 192.168.1.1	dress End IP	Address Su	bnet Mask	Edit	:
) : 4	Source So	PC2	er Address T Single Single	ype Start IP Ad 192.168.1.1 192.168.1.1	dress End IP 1 2	Address Su	bnet Mask	Edit	
) : 4	Source Source	Profile PC1 PC3	er Address T Single Single Single	ype Start IP Ad 192.168.1.1 192.168.1.1 192.168.1.1	dress End IP 1 2 3	Address Su	bnet Mask	Edit × ×	
	Source Source Source Source Source Source	poing Country Filt ce IP urce IP Object Profile PC1 PC2 PC3 urce IP Group	er Address T Single Single Single	ype Start IP Ad 192.168.1.1 192.168.1.1 192.168.1.1	dress End IP 1 2 3	Address Su	bnet Mask	Edit	
	Source Source Source Source Source Source	poing Country Filt ce IP arce IP Object Profile PC1 PC2 PC3 arce IP Group arce User Profile	er Address T Single Single Single	ype Start IP Ad 192.168.1.1 192.168.1.1 192.168.1.1	dress End IP I 2 3	Address Su	ibnet Mask	Edit X X	
	Source Source Source Source Source Source Source Source Source	poing Country Filt The IP Object Profile PC1 PC2 PC3 Urce IP Group Urce User Profile Urce User Group	er Address T Single Single Single	ype Start IP Ad 192.168.1.1 192.168.1.1 192.168.1.1	dress End IP 1 2 3	Address Su	bnet Mask	Edit	
	Source Source Source Source Source Source Source Source Source Source	Profile PC1 PC2 PC3 PC3 PC3 PC3 PC3 PC3 PC3 PC3 PC3 PC3	er Address T Single Single Single	ype Start IP Ad 192.168.1.1 192.168.1.1 192.168.1.1	dress End IP 1 2 3	Address Su	bnet Mask	Edit X X	

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 \vee				
	Next Group :		~				
	SysLog :	) Enable	Disable				
In	put Interface :	ALL LANS	~				
Out	tput Interface :	ALL WANS	~				
If no	object is select	ed in a category	the case of 'Any' is	applied			
	Firewall Ohie	icte	, the case of Any is	applied			
	Time Schedul	P					
	Service Proto	col					
	ncoming Cou	ntry ritter					
	Source ID	Intry Filter					
1	Source IP Ob	ject					
	Profile		Address lype	Start IP Address	End IP Address	Subnet Mask	Edit
	PC1		Single	192.168.1.11			×
	PC2		Single	192.168.1.12			×
	PC3		Single	192.168.1.13			×
₽	Source IP Gro	pup					
₽	Source User	Profile					
₽	Source User	Group					
₽	Source LDAF	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.

F	irewall >> Filter	Setup >> Applic	ation Filter			
Γ	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						
1 1	IP Filter	IPv6 Filter	Application Filter	URL/Web Category Filter	QQ Filter	Default Policy

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