

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.

😋 Add 🛛 🗶	Edit 🛄 De	elete 🗳 Refresi	h 🕋 Move U	p 🛛 🐣 Move Dow	vn 🕻 🔓 Re	Cb Rename Profile Number Limit : 25						
Profile	Enable	WAN Profile	Use IP Alias	Alias F	Private IP		Protocol	Port Redire	Public Port	Public Port	Private Port	
нттр	true	wan1	No	192.168.1.6		6 TCP		One-to-One	80		80	
			Port R Pr W/ Us Pr Pr Po	edirection ofile : Denable AN Profile : e IP Alias : ivate IP : otocol : ort Redirection	H [[[]]]]]]]	TTP wan1 lo 192 . 168 TCP Dne-to-One						



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

Objec	cts Setting >> IP Object					2
	IP Object					
	🚯 Add 🔀 Edit 🏢 De	lete 🗳 Refresh				Profile Number Limit: 200
	Profile	Address Type	Start	IP Address	End IP Address	Subnet Mask
1	HTTP_server	Single	192.1	68.1.6		
2	PC_remote	Single	99.99	.99.12		
						1
		IP Obje	ect		- ×	
		Pro	ofile :	HTTP_server		
		Ad	dress Type :	Single	~	
		Sta	art IP Address :	192 . 168 . 1	1 . 6	
		IP Obje	ect		-×	
		Pro	ofile :	PC_remote		
		Ad	dress Type :	Single	*	
		Sta	art IP Address :	99 . 99 . 9	99 . 12	



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.

IP Filter IPv	6 Filter Application F	ilter URL/Web Cat	egory Filter QQ Filter	Default Policy				
🚯 Add 🛛 🗶 E	dit 📺 Delete 🗳	Refresh 🛛 👉 Mo	ove Up 🛛 🦊 Move Down					Profile Number Li
Group			Enable			Comment		
WAN_LAN			true					
🚺 Add	🗶 Edit 🛛 🕅 Delete	🤝 Refresh 🔾	a Rename 🛛 🍲 Move U	p 🛛 🐣 Move Do	wn			Profile Number Limit : 2
Rule	Enable	Action	Next Group For	Syslog	Source LDAP Gr	General Firewall	Source Firewall	Destination Fire
PC pass	true	accept		Disable			PC_remote	HTTP_server

Reguła 'PC_pass' – przepuszczanie ruchu od zdalnego PC do serwera HTTP

Rule							
	Profile : PC_pass						
	Cinable Enable						
	Action : Accept	*					
	Next Group :	¥					
	SysLog : 💿 Enable	Disable					
In	nput Interface : ALL WANS	*					
Out	tput Interface : ALL LANS	~					
16							
IT NO	Discussion object is selected in a categor	ry, the case of Any is a	pplied				
	Firewall Objects						
	lime Schedule						
	Service Protocol						
	Incoming Country Filter						
	Source IP						
	Drofile	End ID Address	Subpot Mask	Edit			
		Sincle	Start IP Address	192 168 1 6			
	RIIP_server	Single	192.100.1.0			×	
	V PC_remote	Single	39.99.99.12				
₽	Source IP Group						
₽	Source User Profile						
₽	Source User Group						
►	Source LDAP Group						
	Destination IP						
4	Destination IP Object						
	Profile	Address Type	Start IP Address	End IP Address	Subnet Mask	Edit	
	HTTP_server	Single	192.168.1.6			×	
	PC_remote	Single	99.99.99.12			×	
₽	Destination IP Group						
►	Destination DNS Object						
►	Destination User Profile						
►	Destination User Group						
►	Destination LDAP Group						



Requia	'ANY	block'	– hlokowan	ie ruchu	od dowo	lneao ur	rzadzenia	do serwera	HTTP
Regula		DIOCK	DIOROWAII	ic ruciiu	ou uowe	nincyo ui	IZQUZCINU		

Rule											
		Profile :	ANY_block								
			Enable								
		Action :	Block	~							
	Nex	ct Group :		~							
		SysLog :	Enable (Disable							
Ir	nput li	nterface :	ALL WANS	~							
Ou	tput li	nterface :	ALL LANS	~							
If no (objec	t is select	ed in a category	, the case of 'Any' is a	plied						
	Fire	ewall Obje	ects								
± 1	Time Schedule										
+ 5	I Service Protocol										
± I	Incoming Country Filter										
+ (Dut-g	joing Cou	untry Filter								
+ 5	Sourc	ce IP									
- 0)esti	nation IP									
4	Des	stination IP	Object								
		Profile		Address Type	Start IP Address	End IP Address	Subnet Mask	Edit			
		HTTP_se	rver	Single	192.168.1.6			×			
		PC_remo	te	Single	99.99.99.12			×			
►	Des	stination IP	Group								
►	Des	stination D	NS Object								
►	Des	stination U	ser Profile								
►	Des	stination U	ser Group								
	Des	stination L	DAP 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.





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.

IP Filter	IPv6 Filter	Application Filter	URL/Web Category	Filter QQ Filter	Default Policy				
🟠 Add	🔀 Edit 👔	👖 Delete 🛛 🗳 Ref	resh 🛛 👉 Move Uj	o 🛛 🦊 Move Down					Profile Number Limit
Group				Enable			Comment		
WAN_L	AN			true					
()	kdd 🔀 Edii	<u> </u> Delete 🗲	Refresh 🔓 Re	name 🛛 👉 Move Uj	p 🛛 🐣 Move Down				Profile Number Limit: 20
Rule	E	nable A	ction	Next Group For	Syslog	Source LDAP Gr	General Firewall	Source Firewall	Destination Fire
ANY_blo	ck_if tr	ie p	ock_if_no_further	WAN_LAN_excepti	Enable				HTTP_server
	AN excentions			true					
WAN_L	-in_exceptions		- 2	nama 🛆 Maua III	n 🔍 Move Down				Profile Number Limit: 20
WAN_L	kdd 🔀 Edi	前 Delete 🔇 📢	Refresh 🔓 Re	name Trance of					
WAN_L	Add 🔀 Edi	mable A	Refresh GB Re	Next Group For	Syslog	Source LDAP Gr	General Firewall	Source Firewall	Destination Fire

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.

Rule										
		Profile : ANY_bl	ock_if							
		V Ena	ble							
		Action : Block_I	f_No_Further_M 👻							
	Nex	t Group : WAN_L	AN_exceptions							
	SysLog: 🔞 Enable 🔘 Disable									
Ir	Input Interface : ALL WANS									
Ou	Output Interface : ALL LANS									
lf no	no object is selected in a category, the case of 'Any' is applied									
	Firewall Objects									
1	Time Schedule									
•	Servi	ce Protocol								
۰	ncor	ning Country Fil	ter							
+ (Dut-g	joing Country Fi	lter							
H :	Sour	ce IP								
	Desti	nation IP								
4	Des	stination IP Object								
		Profile	Address Type	Start IP Address	End IP Address	Subnet Mask	Edit			
		HTTP_server	Single	192.168.1.6			×			
		PC_remote	Single	99.99.99.12			×			
▶	Destination IP Group									
₽	Destination DNS Object									
₽	Des	stination User Prof	ile							
₽	Des	stination User Grou	up							
₽	Des	stination LDAP Gro	oup							



Grupa 'WAN_LAN_exceptions' reguła 'PC_pass' – przepuszczanie ruchu od zdalnego PC do serwera HTTP

ule							
Profile	: PC_pass						
	Enable						
Action	Accept	~					
Next Group	:	~					
SysLog	: O Enable (Disable					
Input Interface	ALL WANS	*					
Output Interface	: ALL LANS	~					
6							
Firewall O	cted in a category	y, the case of Any is a	appiled				
	ule						
Service Prof							
	untry Filter						
Incoming co Out-going C	ountry Filter						
Source IP							
Source IP Object							
Profile		Address Type	Start IP Address	End IP Address	Subnet Mask	Edit	
HTTP_	server	Single	192.168.1.6			×	
PC_rer	note	Single	99.99.99.12			×	
Source IP C	Group						
Source Use	er Profile						
Source Use	er Group						
Source LD/	AP Group						
Destination	IP						
Destination	IP Object						
Profil	e	Address Type	Start IP Address	End IP Address	Subnet Mask	Edit	
☑ HTTP_	server	Single	192.168.1.6			×	
PC_rer	note	Single	99.99.99.12			×	
Destination	IP Group						
Destination	DNS Object						
Destination	User Profile						
Destination	User 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.

Fin	ewall >> Filter	Setup >> Defau	It Policy			0				
	IP Filter	IPv6 Filter	Application Filter	URI /Web Category Filter	00 Filter	Default Policy				
11										
	Hap Default Deliau : Assest									
	use Detau	Acce	pt	•						

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