



Główne założenia:

- PPTP Host-LAN
- Klient VPN ma dostęp tylko do Serwera 192.168.0.10 brak dostęp do pozostałych urządzeń w podsieci 192.168.0.0/24

Przejdź do zakładki **User Management>>User Profile>>User Profile**. Stwórz odpowiedni profil użytkownika.

🖏 Add	🗶 Edit 🕅 I	Delete 🗳 Refr	resh									Profile Numb	er Limit : 5
Usern	ame Enable	System U	Allow Web	Time Quota	Remainin	g Time	PPTP Dial-in	L2TP Dial-in	SSL Tunnel	Use mOTP	Allow PPP	Time Quot	Traffic
test	true	false	Disable	Disable	1440	Recharge	Enable	Disable	Disable	Disable	Disable	0/-1	0/-1
											_		
		User	Profile								×		
		llee			toot					-			
		USER V F	Fnable		lesi								
		Daes	aword :					1					
		Pass	sword.]					
		Syst	em user :		false		*						
		^	User Manage	ement									
		\sim	PPTP/L2TP/P	PPoE Server									
		Idle	Timeout(se	ec):	300			(PPTP/L2TP	/PPPoE/SSL	Server)	-		
		PPT	P Dial-in :		i Ena	able 🦱	Disable			-			
		1.271	Dial in :		© En	abla @	Diaabla						
		LZII	P Dial-III .			able 🎯	Disable						



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

Ob	ects	Setting >> IP Object				2
	IP	' Object				
	đ	👌 Add 🛛 🔀 Edit 🛚 👖 Delete	📢 Refresh			Profile Number Limit : 200
		Profile	Address Type	Start IP Address	End IP Address	Subnet Mask
	1	subnet_local	Subnet	192.168.0.0		255.255.255.0
	2	server_local	Single	192.168.0.10		
	I	P Object			Object	
		Profile : s	ubnet_local		0.0,000	
		Address Type :	Gubnet 🗸		Profile : server_loca	I
		Start IP Address :	192 . 168 . 0 . 0		Address Type : Single	×
		Subnet Mask : 2	\$55.255.255.0/24		Start IP Address : 192 . 1	. 0 . 10

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

IP Filter IPv6 F	itter Application Filter	URL/Web Category Fi	ter QQ Filter I	Default Policy				
🕼 Add 🛛 🗶 Edit	<u> n</u> Delete 🛛 📢 Ref	iresh 🕋 Move Up	🦊 Move Down				Pr	rofile Number Limit :
Group			Enable			Comment		
vpn_control			true					
🕼 Add 🔀	Edit <u> </u>	Refresh 🔓 Rena	me 🔺 Move Up	🐣 Move Down				Profile Number Li
Rule	Enable	Action	Next Group For F	Syslog	Source LDAP Gro	General Firewall	Source Firewall T	Destination Firev
	1			Disable			test	server local
PPTP_user_pass	true	pass		Disable			toot	oonton_loodi



Rule															
	Profile :	PPTP use	er pass												
		Enab	le												
	Block Action :	Pass		~	Î										
	Next Group :			~	1										
	Cuel es :	C Ench		iachla											
	SysLog :	Cinar	bie 🎯 D	Isable	ĩ										
In	iput Interface :	Any		*											
Out	tput Interface :	Any		~											
While	e no target has	been spe	cified, fire	wall rules	are applie	d to Any o	bject								
	Firewall Obj	ects													
- 1	Fime Schedu	le													-
₽	Time Object														
₽	Time Group														
Ξ \$	Service Proto	col													
₽	Service Type	e Object													
₽	Service Type	e Group													
	ncoming Cou	untry Filte	r												
₽	Source Cour	ntry Object	(At most	accept 15	countries)									
Ξ (Out-going Co	untry Filt	er												
	Destination C	Country Ob	ject (At m	nost accept	15 count	ries)									
	Source IP														
	Source IP Ob	oject													
	Source IP Gr	oup													
4	Source User	Profile				-									
	User	Enable	Syst	Allo	Time	Rem	PPTP	L2TP	SSL	Use	Allo	Time	Traffi	Edit	
	V test	true	false	Disable	Disable	1440	Enable	Disable	Disable	Disable	Disable	0/-1	0/-1	X	
₽	Source User	Group													
₽	Source LDA	P Group													
	Destination IF)													
4	Destination I	P Object													
	Profile		A	ddress T	ype	Start I	P Addres	ss	End IP Ad	dress	Sub	net Mask		Edit	
	subnet_	local	SI	ubnet		192.16	8.0.0				255.2	255.255.0		×	
	server_	local	Si	ingle		192.16	8.0.10							×	
₽	Destination I	P Group													
►	Destination D	NS Object	t i												
►	Destination U	Jser Profile	•												
►	Destination U	lser Group)												
₽	Destination L	DAP Grou	р												



Rule															
	Drofile		vr. black												
	Profile :	FriP_use	le												
	Block Action :	Black		~	1										
	Next Group :	DIOCK													
	Next Group .														
	SysLog :	Enat	ole 🎯 🛛	isable	1										
Ir	nput Interface :	Any		~											
Ou	tput Interface :	Any		~											
While	e no target has	been spe	cified, fire	wall rules	are applied	d to Any o	bject								
	Firewall Obj	ects													
	Time Schedu	le													[
₽	Time Object														
₽	Time Group														
•	Service Proto	col													
₽	Service Type	e Object													
₽	Service Type	Group													
	ncoming Cou	untry Filte	er												
₽	Source Cour	ntry Object	(At most	accept 15	countries))									
- (Dut-going Co	untry Filt	er												
	Destination C	Country Ob	ject (At n	nost accep	t 15 countr	ries)									
-	Source IP														
	Source IP Ob	oject													
₽	Source IP Gr	oup													
4	Source User	Profile		1202							2.2				
	User	Enable	Syst	Allo	Time	Rem	PPTP	L2TP.	. SSL	Use	Allo	Time	Traffi	Edit	
	V test	true	false	Disable	Disable	1440	Enable	Disable	Disable	Disable	Disable	0/-1	0/-1	×	
₽	Source User	Group													
₽	Source LDA	P Group													
- (Destination IF	0													
4	Destination I	o Object													
	Profile		A	ddress T	ype	Start	P Addres	ss	End IP Ad	dress	Sub	net Mask		Edit	
	v subnet	local	S	ubnet		192.16	8.0.0				255.3	255.255.0		×	
	server_	local	S	ingle		192.16	8.0.10							×	
₽	Destination I	Group													
₽	Destination D	NS Object	t)												
₽	Destination U	Iser Profile	•												
₽	Destination U	lser Group													
₽	Destination L	DAP Grou	D												



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.

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>