This is how you block an attacking public IP from the outside:

Log onto your firewall and do the following:

1. Click on Objects  $\rightarrow$  address book  $\rightarrow$  interface addresses  $\rightarrow$  add  $\rightarrow$  IPv4 address.



2. Under the General tab, name your "attacker" IP and specify the "attacker's" IP.

Use an IP4 Address item to define a name						
General User Authentication						
췶 Gener	al					
Name:	Name: Attacker_IP					
Address:	196.25.190.226					
A. c	4-					

3. Then it should look like this:

6	An address folder can be used to group related address objects for better overv							
	<b>`</b> ]-	Add - Edit this object						
	Na	me 🚽	Address 🚽					
	ß	Attacker_IP	196.25.190.226					
	Ŗ	dmz_ip	172.17.100.254					
	ę	dmznet	172.17.100.0/24					
	P	lan_ip	192.168.1.1					
	ę	lannet	192.168.1.0/24					
	9	wan_br	0.0.0.0					
	9	wan_dns1	0.0.0.0					
	9	wan_dns2	0.0.0.0					
	9	wan_gw	0.0.0.0					
	9	wan_ip	0.0.0.0					
	9	wannet	0.0.0/0					

4. Now we need to add an IP rule to block that IP. Click on Rules → IP Rules and under the General tab, name your rule = drop-public-ip, Action = Drop, Service = all\_services. Your address filter will be as follows: Interface source = wan1, Network source = attacker\_ip, Interface destination = any and Network destination = all-nets.

	8 IP F	Rule		
DFL-860 Dobjects Debject	An IP Genera Marne: Action: Service: Schedule:	I Log Settings Log Settings al drop-public-ip Drop all_services (None)	ion to perform on network tr	Multiplex SAT SL
E ZoneDefense	Specify so	urce interface and sour Source	ce network, together with de Destination	estination interface and de:
	Interface:	wan1	✓ any	~
	Network	attacker ip	✓ all-nets	~

5. Now you need to move your IP rule to the top of the list. Right-click the rule and select Move to Top.

8	IP Rules	P-based	d network traffic	. In addition, th	hey provide me	ans
÷٩,	Add 🖵					
-	Na			Action		Sec
1	8	pina	fw	Action Allow		153
2	, i i i i i i i i i i i i i i i i i i i	lan_t	:o_wan			
3	8	d C	Edit	Drop		<b>19</b> 90
		×	Delete			
		11	Disable			
		1	Move to Top			
		-	Move Up			
		۲	Move To			
		- 🕓	Move Down			
		- 🕓	Move to Botto	n		

6. Now it should look like this:

8	IP Rules IP rules are used to filter IF	P-based network traffic.	In addition, they provide me	eans for address translation a	as well as Server Load Bala	ncing.
Pa Ad	dd 🗸					
#	Nar	me	Action	Src If	Src Net	Dest
1	\$	drop-public-ip	👓 Drop	🔝 wan	😽 Attacker_IP	- 193 a
2	\$	ping_fw	🟦 Allow	🔢 lan	🗟 lannet	53 c
3	C	lan_to_wan				

7. Save and activate and you are done. Your network will now be safe from that attacking public IP.

🌎 Home 🛛	🔣 Configuration -	Ti I	ools 🚽 📔	👩 Status 🗸	Naintenance 🗸
	Save and Activate				
	🛃 Discard Changes	_	8	<b>IP Rules</b>	
🗟 DFL-210	🛃 View Changes		•	IP rules are used	to filter IP-based network traf
🗄 🕖 🧑 System					