A Zorp Gateway szolgáltatást kiegészítő DDoS elleni biztonsági megoldás

2022. július 28.

A cél olyan értéknövelő szolgáltatás keresése volt, amely a <u>Zorp Gateway</u> alapú határvédelmet kiegészíti egy DDoS (Distributed Denial of Service) elleni védelemmel. A következőkben leírjuk a Fail2ban, *Zorp*ot kiegészítő szolgáltatásának használatával kapcsolatos tapasztalatokat.



Szerzői jog © 1996-2022 BalaSys IT Ltd.

Tartalom

1. A probléma bemutatása	
2. A megoldás bemutatása	
3. Technikai megvalósítás	
3.1. Telepítés	
4. Konklúzió	

Egyre többször fordulnak elő túlterheléses támadások (Distributed Denial of Service, DDoS), amelyeknek súlyos következményei lehetnek vállalatunk vagy márkánk hírnevére is, ha például weboldalunk hosszabb időre elérhetetlenné válik miattuk. Szélsőséges esetben üzletkritikus vagy stratégiai szolgáltatások (pl. energia, távközlés) megbénítására is irányulhatnak az ilyen támadások, ezért a célzott védekezés ellenük ma már alapvető követelmény.

2. A megoldás bemutatása

A *Fail2ban* egy szabadon használható, Unix/Linux alapú behatolásmegelőző program, ami képes a logokban megkeresni a sikertelen login próbálkozásokat, illetve ez alapján a kliens IP címét meghatározni, majd erre egy netfilter szabályt létrehozva igyekszik a potenciális támadást kivédeni.



Megjegyzés Rövid tesztidőszakunk alatt a 2222-as portra irányuló forgalom került szűrésre.

Az alábbiakban a DDoS támadások kivédésének egy lehetséges technikai módját mutatjuk be a *Zorp Gateway* és a *Fail2ban* integrálásával.

3. Technikai megvalósítás

A célunk az volt, hogy a meglévő határvédelmi szolgáltatások mellé egy könnyen illeszthető, a felhasználói igényeket is kielégítő, DDoS elleni védelmet biztosítsunk. A tesztidőszak alatt az SSH (Secure Shell) forgalom kerüljön szűrésre egyszemélyes használattal.

3.1. Telepítés

Esetünkben az Ubuntu Universe tárolóból érhető el a Fail2ban csomag:

```
# cat /etc/apt/sources.list
    deb http://at.archive.ubuntu.com/ubuntu bionic main universe
```

Az Ubuntu csomagkezelő szoftver, az apt eszköz segítségével telepíthető:

```
$ sudo apt update$
sudo apt install fail2ban
```

3.1.1. Konfigurálás a Zorp Management Console segítségével

A konfigurálás az /etc/fail2ban/jail.local fájl szerkesztésével lehetséges.

1. Hozza létre az /etc/fail2ban/jail.local fájlt a telepítést követően a jail.conf fájl másolásával:

\$ sudo cp /etc/fail2ban/jail.conf /etc/fail2ban/jail.local

- 2. Olvassa be .conf fájlt a *Fail2ban*. Ha létezik .local fájl, akkor az abban lévő tartalom felülírja az eredeti, általános tartalmat.
- 3. Tegye szerkeszthetővé a jail.conf fájlt a *Zorp Management Console (ZMC)* segítségével. Ehhez free text plugint tudunk használni.
- 4. Vegyen fel egy új *Free text plugint* az alábbi módon: *Új/Text editor/Text editor minimal*

Három adatot kér a felület: komponens neve, a konfigurációs fájl, systemd service neve.

					Zorp Manage	ement Co		- admin@	0172.10	5.12.202					
File Edit View Config	uration	Manag	gemen	nt PKI	Help										
Configuration		L	• • •	·•••	₹ 🗘	¢, _	$\widehat{}$	-	-	•?•	••	옙			
Default_Corporate		Host	Ргоре	erties	Quarantine										
R Management ag	ents	Host	nanad	remen	F										
R Management se	erver	moser	nanaş	gemen											
R Networking		Syste	m												
Packet filter		_			Z	MC - Add	l new d	ompone:	nt				8		
Zorp								_							
	Comp	onen	ts av	ailabl	e										
		16			ZMC -	Add com	ponen	t from te	mplat	e		8	â		
	nt	Netwo	Com	ponent	variables								VPN		
				. 1	lext compon	ent name	Fail2t	Dan				•			
				Comp	onent config	file name	/etc/	fail2ban/j	ail.loc	al		-			
	Compo	nent t	Com	ponent	systemd serv	/ice name	fail2t	oan.servio	e			-			
	Descrip	ption													
	Text ed	itor mir r													
	Domain	s Name													
	Domain	Name													
	Packag	e sourc													
									M	legse		ОК			
														Managem	ent connection
												Méase	ОК	ection	Shutdown
F		Compo	nents	in use											
			φ.,			67		ĩđ		F	3				
		Manao	gemen	it agents	a Managerr	ਝਾ 1ent serve	ir N	ریں etworkir	ng	Packe	E) t filter		Zогр		
				2					2				·		
		Új		Törlés											Configure
Committed															

1. ábra - Free text plugin felvétele

5. Töltse be a host-on/node-on lévő másolatot a *ZMC* felületére a *Download file* gomb segítségével.

\$

	Zorp Management Console - admin@172.16.12.202	000
File Edit View Configuration	n Management PKI Help	
Configuration	토 😔 😔 🖻 🗗 💮 📀 ④ 🚹 🗄 🖬 🔍	
Default_Corporate TMS_Host	/etc/fail2ban/iail.local	
R Management agents	# WARNING: heavily refactored in 0.9.0 release. Please review and	
R Management server	# Customize settings for your setup. # Channel, in most of the earce you should not medify this	
Networking	<pre># file, but provide customizations in jail.local file, # or senarate conf files under jail d/ directory e a ;</pre>	
R Packet filter	# HOW TO ACTIVATE TATLS:	
R Zorp	# # YOU SHOULD NOT MODIFY THIS FILE.	
TUREDUN	# It will probably be overwritten or improved in a distribution update. # drawida supportions in a juli local file on a juli d/supportion local	
	Provue customizations in a jail.uccal file or a jail.org/ustomisation.local. For example to change the default bantime for all jails and to enable the # ssh-iptables jail the following (uncommented) would appear in the .local file. & See man 5 jail.comf for details.	
	# [DEFAULT] # bantime = lh #	
	<pre># [sshd] # enabled = true</pre>	
	# # See jail.conf(5) man page for more information	
	# Comments: use '#' for comment lines and ';' (following a space) for inline comments	
	[INCLUDES]	
/	#before = paths-distro.conf before = paths-debian.conf	
	<pre># The DEFAULT allows a global definition of the options. They can be overridden # in each jail afterwards.</pre>	
2	[DEFAULT]	
	# MISCELLANEOUS OPTIONS #	
	<pre># inporself* specifies whether the local resp. own IP addresses should be ignored # (default is true). FailZban will not ban a host which matches such addresses. #ignorself = true</pre>	
	<pre># "ignoreip" can be a list of IP addresses, CIDR masks or DNS hosts. Fail2ban # will not ban a host which matches an address in this list. Several addresses # can be defined using space (and/or comma) separator. #ignoreip = 127.0.0.1/8 ::1</pre>	
	<pre># External command that will take an tagged arguments to ignore, e.g. <ip>, # and return true if the IP is to be ignored. False otherwise.</ip></pre>	
	# ignorecommand = /pain/io/command <lp></lp>	
Unsaved changes		

2. ábra - A másolat betöltése

6. Módosítson két sort, és adjon hozzá egy sort a *jail.local* sshd részhez, ahogy a következő diff fájl mutatja:

```
< port = ssh
< logpath = %(sshd_log)s
---
> enabled = true
> port = 2222
> #logpath = %(sshd_log)s
> logpath = /var/log/messages
```

Ezzel engedélyezzük az sshd logjainak vizsgálatát, amit a üzenetekbben talál a *Fail2ban*. A szolgáltatást célszerű engedélyezni:

```
$ sudo systemctl service enable fail2ban
```

Érdemes a fájlok jogosultságát 644-es értékre visszaállítani, illetve a *fail2ban-client státusz* is jól használható.

Zorp M	anagement Console - admin@172.16.12	2.202	
File Edit View Configuration Management PKI Help			
	<u>, i ()</u> () () () () () () () () () () () () ()	1 Q	
Default_Corporate /etc/fail2ban/jail.local			
R Management agents # Report block via blocklist.de	fail2ban reporting service API		
R Manage	ZMC - Files		
R Networ Configuration Scripts			
M Fail2bar Configuration files			ban_agent)s"]
Filename 👻 Owner Grou	ip Mode Manage		
/etc/fail2ban/jail.local root root	0644 🗹		
File settings			
Filename: /etc/fail2ban/jail.local			
Mode: 0644	Owner: root	Group: root	
Consider different if these properties	change		
Mode Owne	er 🔽 Group	🗹 Checksum	
Size Modi	fication time 🛛 🗹 Status modifica	tion time 🛛 🗹 Inode	
Check All Uncheck All			
Postprocess script			
Postprocess command: /usr/bin/fa	ail2ban-client status	Végrehajtás	
		Mégse OK	
enabled = true port = 2222 #logpath = %(sshd_log)s logpath = √var/log/messages backend = %(sshd_backend)s [dropbear]			

3. ábra - Fail2ban

\$

	Run o	command			●
File Edit					
Wed Mar 6 15:10:56 2019					
Postprocess script '/usr/bin/fail2ban-cl	ient status' or	n host 'ZMS-Host	:': succeeded		
Standard output: Status - Number of jail: 1 `- Jail list: sshd					
	Mentés	Keresés	Törlés	Dock	Bezárás

4. ábra - Fail2ban-client státusz

\$

4. Konklúzió

A fenti megoldás könnyen beilleszthető a *Zorp* központi menedzsment felületére és megbízható kiegészítő szolgáltatást nyújt a DDoS elleni védekezéshez. A rendszer használatának előnye, hogy rugalmas, sok lehetőséget biztosít. A figyelt szolgáltatások és azok portjai könnyen meghatározhatóak a szöveges konfigurációs állományban. A *ZMC* free text pluginját használva központilag menedzselhető. Növelheti azonban a fájlok karbantartásához szükséges időt. A telepítés és konfigurálás után további adminisztrációra, a beállítások finomítására lehet szükség.



Megjegyzés Odafigyelést igényel, nincs hozzá a *ZMC-ben* specifikált felület.