A *Zorp Gateway* szolgáltatást kiegészítő DDoS elleni biztonsági megoldás

2022. július 28.

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

Tartalom

1. A probléma bemutatása

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

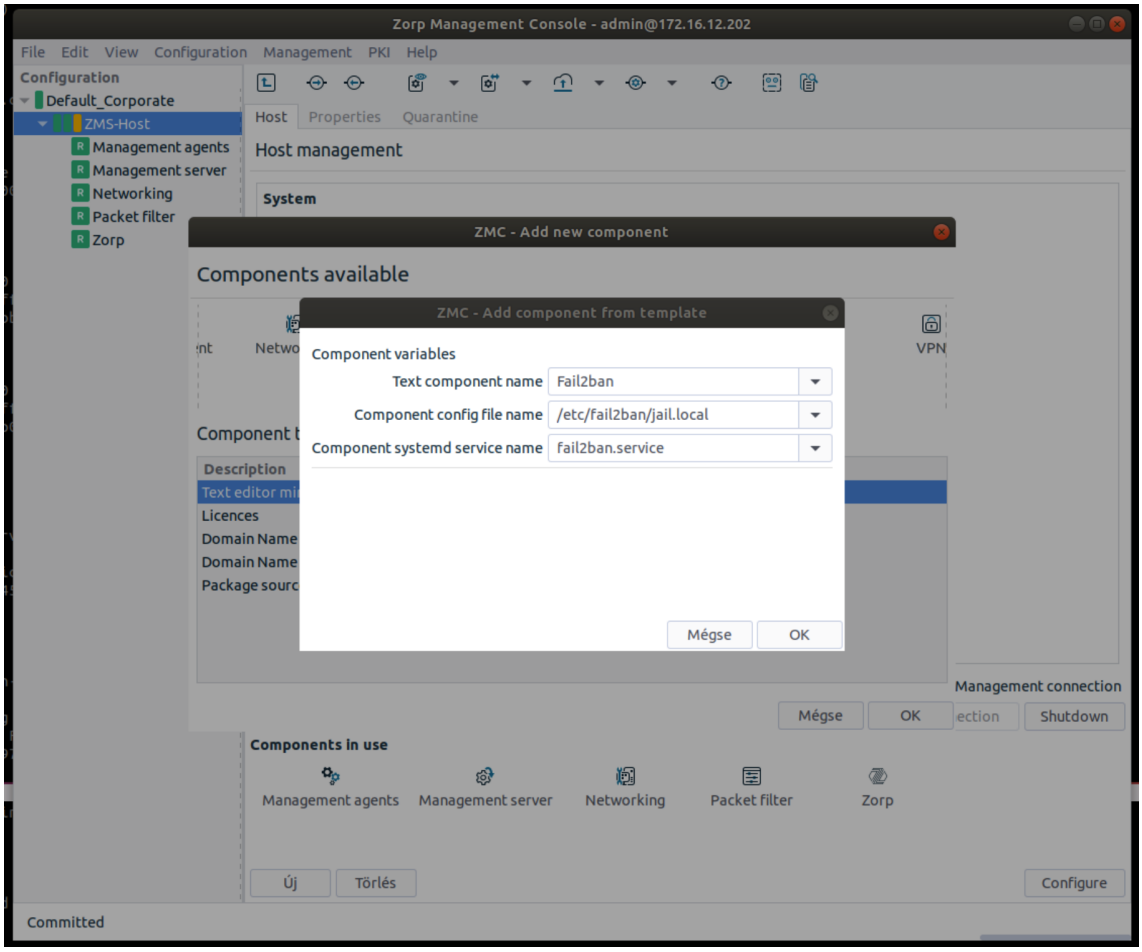
A konfigurálás az */etc/fail2ban/jail.local* fájl szerkesztésével lehetséges.

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
   ```

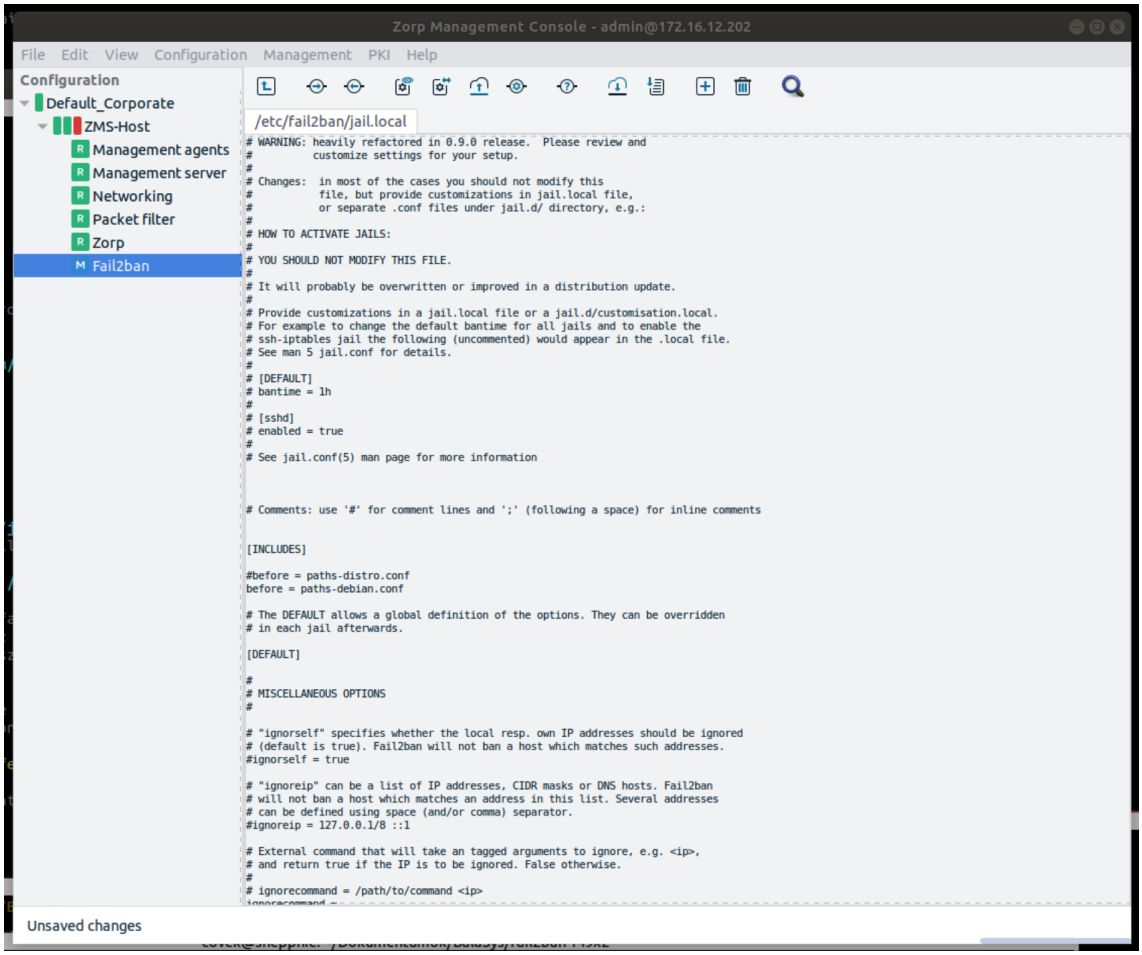
2. Olvassa be `.conf` fájlt a *Fail2ban*. Ha létezik `.local` fájl, akkor az abban lévő tartalom felülírja az eredeti, általános tartalmat.
3. Tegye szerkeszthetővé a `jail.conf` fájlt a *Zorp Management Console (ZMC)* segítségével. Ehhez free text plugint tudunk használni.
4. Vegyen fel egy új *Free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

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



1. ábra - Free text plugin felvétele

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



2. ábra - A másolat betöltése

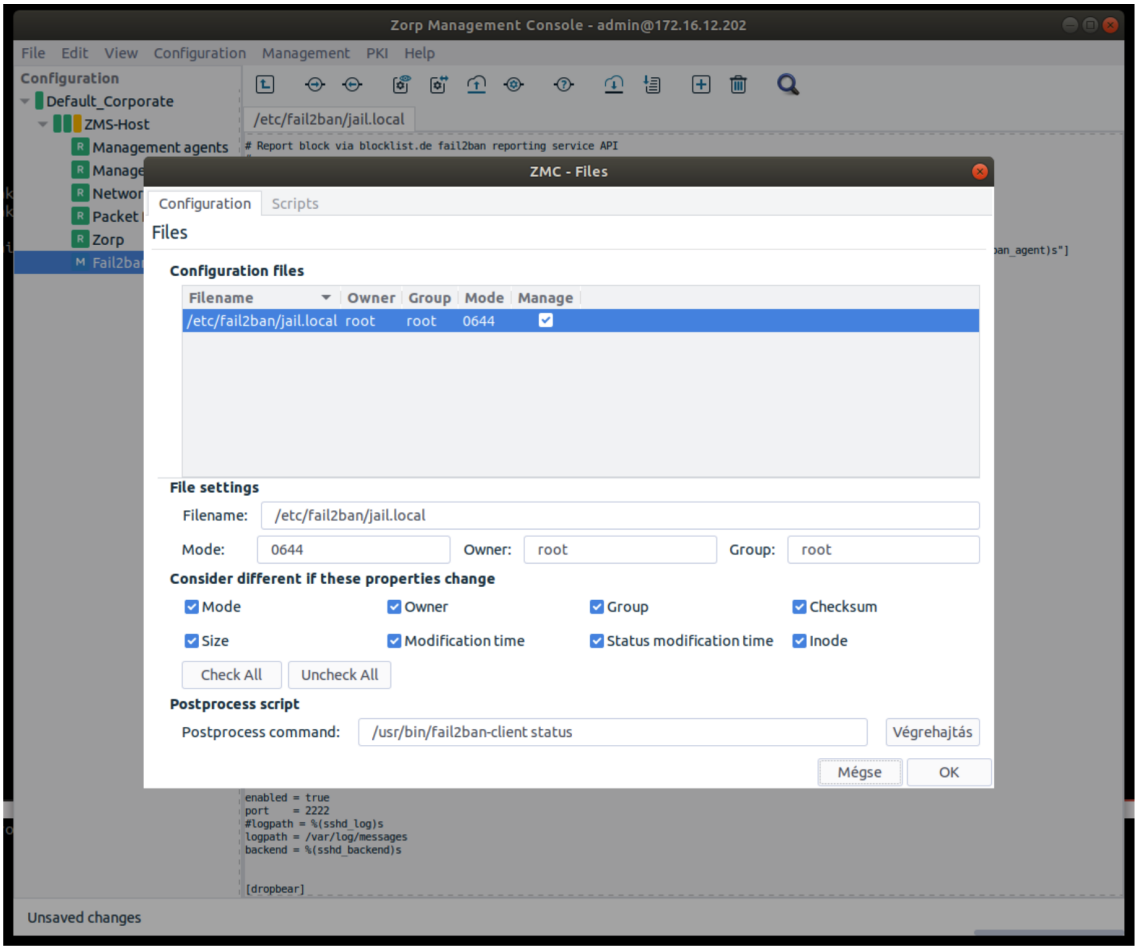
6. Módosítson két sort, és adjon hozzá egy sort a *jail.local* sshd részhez, ahogy a következő diff fájl mutatja:

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

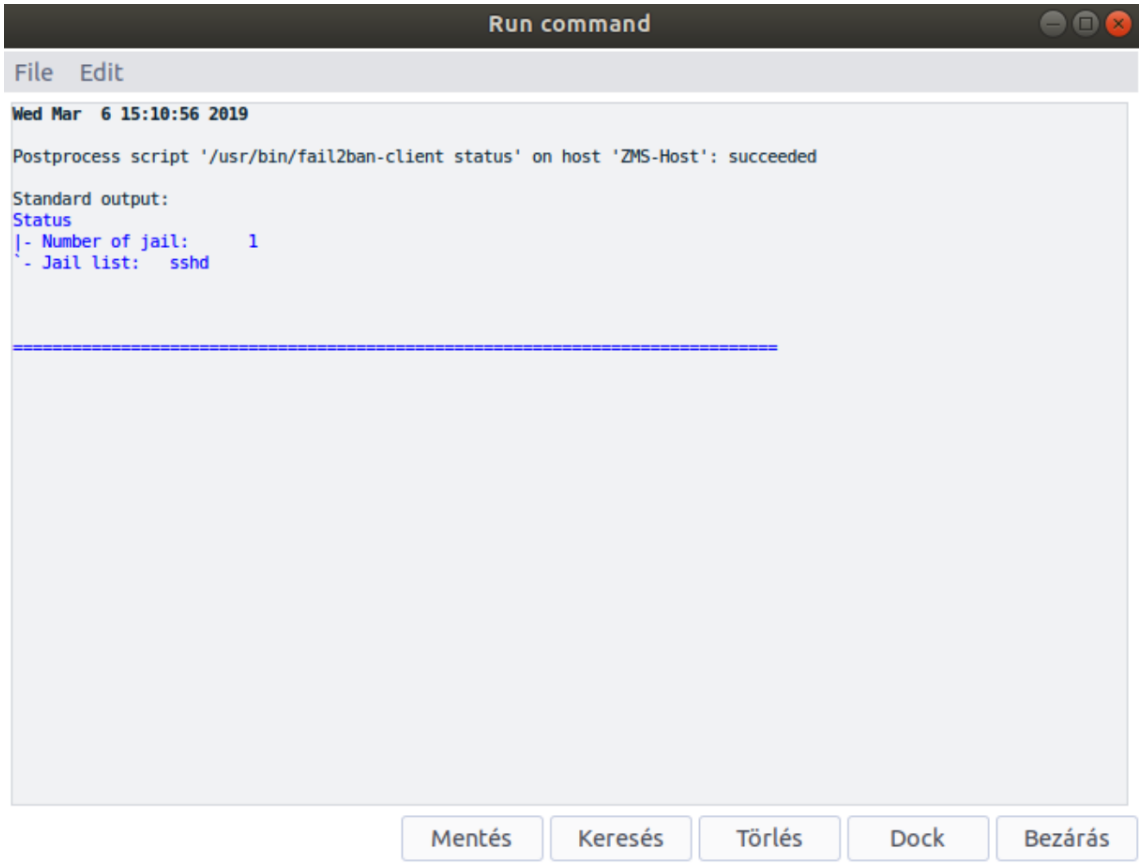
Ezzel engedélyezzük az sshd logjainak vizsgálatát, amit a üzenetekbben talál a *Fail2ban*. A szolgáltatást célszerű engedélyezni:

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

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



3. ábra - Fail2ban



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.