Zorp Gateway tűzfalak központi menedzsmentje SaltStack alkalmazással

2022. július 28.

A megbízhatóbb működés és a hatékonyabb támogatás érdekében a Balasys elsősorban, a *Zorp* saját menedzsment eszköztárát a *Zorp Management Server (ZMS)* és a *Zorp Management Console (ZMC)* használatát javasolja. Nagyvállalati környezetben, több tűzfal használata esetén azonban opcionálisan a *Zorp Gateway* tűzfalak központi menedzsmentjét a *SaltStack* alkalmazás is elláthatja.

Szerzői jog © 1996-2022 BalaSys IT Ltd.

Tartalom

1. A probléma bemutatása

Komplex, nagyvállalati környezetben több tűzfalra is szükség lehet a terheléselosztás és a biztonság növelése érdekében. Nagyszámú, egységes konfigurációval rendelkező tűzfalat (pl. soktelephelyes vállalat) nem hatékony egyesével konfigurálni, hanem valamilyen központi IT automatizációs megoldást célszerű használni.

2. A megoldás bemutatása

Ha egyszerre több, ugyanolyan szabályrendszert használó *Zorp Gateway* tűzfalat kell távolról menedzselni, és a *Zorp Management Server (ZMS)* valamilyen okból nem használható, akkor megoldás lehet egy nyílt forráskódú konfiguráció menedzsment eszköz használata is, mint amilyen a *SaltStack* vagy az *Ansible*.

3. Technikai megvalósítás

A megfelelő *Zorp* komponensek konfigurációs állományainak módosításával, majd a *Zorp* kontroll folyamat (zorpctl) újratöltésével módosíthatók a tűzfalak szabályrendszerei.

3.1. Telepítés

SaltStack használata esetén első lépésben tesztelje, hogy a következő csomagok megvannak-e illetve hiányuk esetén telepítse őket:

- zorp-pro
- zorp product-minimal
- zorp-utils
- zorp-customizer
- zorp-common

Mint a következő példában:

- install-zorp:
- pkg.installed
- pkgs:
  - zorp-pro
  - zorpproduct-minimal
  - zorp-utils
  - zorp-customizer
  - zorp-common

3.2. Konfigurálás

Ellenőrizze, hogy a *Zorp Gateway* működéséhez szükséges fájlok megvannak-e az `/etc/zorp` könyvtárban:

- instances.conf
- license.txt
- policy.py
- zones.py

Ezeknek a fájloknak a tartalmát és szerepét mutatja a következő példa:

- Az *instances.conf* tartalmazza az összes *instance* paraméterét például: instance nevét, log szintjét (loglevel), threads határértékét, core dump készítését stb.:

```
--threads 2000 --process-mode safe-background --enable-core  --verbose 3
--log-spec
           '*.accounting:4,core.summary:4' --log-tags  --uid zorp --gid
zorp --fd-limit-min 256000 --policy
           /etc/zorp/policy.py -- --num-of-processes 1
```

- A *license.txt* tartalmazza a *Zorp Pro licencet*, mely nélkül bár konfigurálható a tűzfal, de a rajta áthaladó forgalmat blokkolja.
- A *policy.py* tartalmazza a szabályrendszert. Ennek a generálására legcélszerűbb a saját GUI-val rendelkező *Zorp Management Consolet (ZMC)* használni, mely segítségével a szabályrendszer létrehozását követően, azt kigenerálhatjuk egy „golden image” tűzfalra. Mint a következő példában:

```
Rule(rule_id=1,
src_zone=('zona1', 'zona2', ),
dst_zone=('zona3', ),
dst_port=(TCP/UDP port number, ),
proto=protocol number,
service='instances_name/service_name'
)
```

- A *zones.py* tartalmazza a zóna szerkezetét, amelyben a cél és a forrás IP címek és DNS nevek vannak definiálva.
  Ahogy a következő példában:

```
Zone(name='zona1',
admin_parent='parent_zone_name',
addrs=[
'1.2.3.4/32',
],
hostnames=[
'FQDN',
]
)
```

- A fent említett fájlokat a következő módon lehet *SaltStack* segítéségével a megfelelő helyre tenni, és a megfelelő jogosultságokkal ellátni:

```
instances.conf:
     filel.managed:
        - name: /etc/zorp/instances.conf
        - user: root
        - group: zorp
        - mode: 640
        - source: /salt_srv_home/instances.conflicense.txt:
     filel.managed:
        - name: /etc/zorp/license.txt
        - user: root
        - group: zorp
        - mode: 644
        - source: /salt_srv_home/license.txtpolicy.py:
     filel.managed:
        - name: /etc/zorp/policy.py
        - user: root
        - group: zorp
        - mode: 640
        - source: /salt_srv_home/policy.pyzones.py:
     filel.managed:
        - name: /etc/zorp/zones.py
```

```
        - user: root
        - group: zorp
        - mode: 640
        - source: /salt_srv_home/zones.py
```

- Amint a konfigurációs állományok a megfelelő helyre kerültek, a *Zorp* kontrol folyamatot újra kell indítani, hogy elkezdje használni az új fájlokat. Ezt a következőképpen lehet megtenni: *zorpctl-restart*:

```
         cmd.run:
              - name: ”zorpctl reload”
              - require:
                   cmd: zorpctl
```

4. Konklúzió

A fenti megoldás a *SaltStackre* alkalmazható, de a megfelelő konfigurációs paraméterek módosításával az *Ansible* használata esetén is működik. A pontos konfiguráció generálásához célszerű egy teszt *Zorp Management Servert* használni, hogy az egyes konfigurációs fájlok szintaktikája megfelelő legyen, majd a tesztrendszerben generált konfigurációt érdemes nagy számban használni valamilyen konfigurációkezelő szoftver segítségével.

A *Zorp* saját eszköztára, a *Zorp Management Server (ZMS)* és a *Zorp Management Console (ZMC)* mellett, nagyvállalati környezetben, több tűzfal használata esetén, megoldást nyújthat a *SaltStack* ismertetett megoldása.