# Webalkalmazás szintű védelem - Web Application Firewall

**2022. július 28.**

**Az alábbi esettanulmány a ModSecurity illesztését vizsgálja *Zorp Gateway-hez*. A *ModSecurity* egy nyílt forráskódú, platformfüggetlen webes alkalmazásszintű tűzfal modul (Web Application Firewall (WAF)). A *ModSecurity WAF* megoldása belelát a HTTP(S) forgalomba, és egy erőteljes szabályleíró nyelvet és API-t biztosít a fejlett védelem megvalósításához. A *ModSecurity* modul a *Zorp Gateway* környezetbe integrálható az alább leírt módon.**

**Szerzői jog © 1996-2022 BalaSys IT Ltd.**

# Tartalom

1. A probléma bemutatása ..... 3
2. A megoldás bemutatása ..... 4
3. Technikai megvalósítás ..... 5
    3.1. Ellenőrzés ..... 12
4. Konklúzió ..... 14

# 1. A probléma bemutatása

A *Zorp Gateway-jel* eddig is lehetséges volt különféle webszervereket védeni SSL terminálás megvalósításával, de a HTTP protokollt ellenőrző proxy az RFC betartásáért, míg a *Zorp Content Vectoring System* NOD32 és egyéb moduljai az átvitt tartalom vírusszűréséért felelnek. Így ezidáig olyan WAF modul nem volt közvetlenül integrálható, ami a webszerverek elleni támadások alkalmazásszintű védelmét oldaná meg.

## 2. A megoldás bemutatása

A *ModSecurity*, a *Zorp* HTTP proxyba a *Zorp Content Vectoring System (ZCV)* modullal beágyazható, és az átvitt HTTP fejlécek és adatok egyidejű elemzésével, a megfelelő szabályminták alapján (ingyenes: „OWASP ModSecurity Core Rule Set (CRS) Version 3” vagy professzionális: „Commercial Rules from Trustwave SpiderLabs”) a webszerver védelmének egy további, független rétegét képezi. A megoldás által a rosszindulatú vagy kockázatos HTTP kérések általában már a *Zorp Gateway-en* fennakadnak, és nem jutnak el a webszerverig.

# 3. Technikai megvalósítás

A *ModSecurity* modult a *ZCV* licenc csak igény esetén tartalmazza. Használatát a licenc vásárlásakor vagy hosszabbításakor külön kell jelezni a Balasys felé.

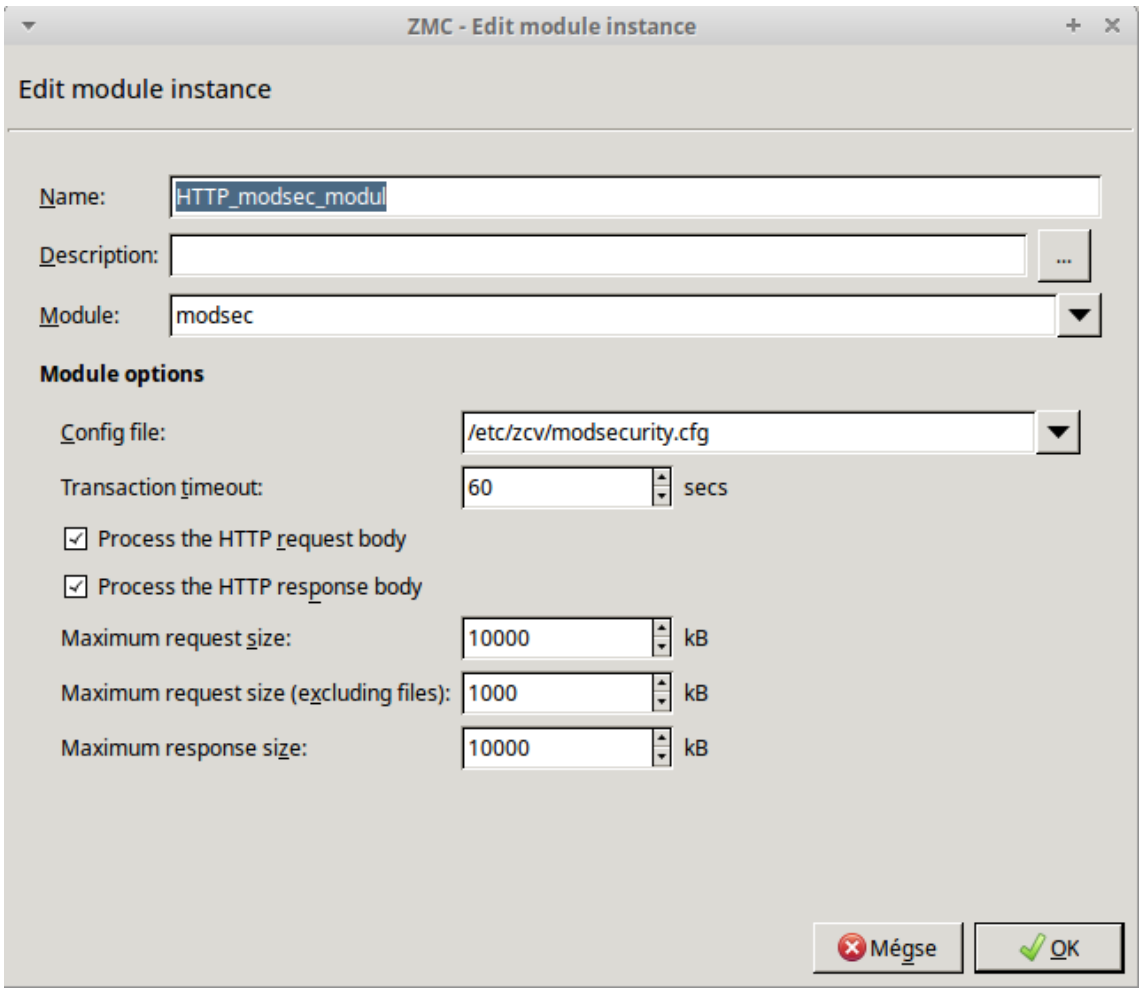
1. Telepítse a megfelelő könyvtárakat és programmodulokat a tűzfalon. Amennyiben még nincsenek meg, az alábbi parancs kiadásával telepítheti:

   ```
   sudo apt install zorpproduct-modsecurity
   ```

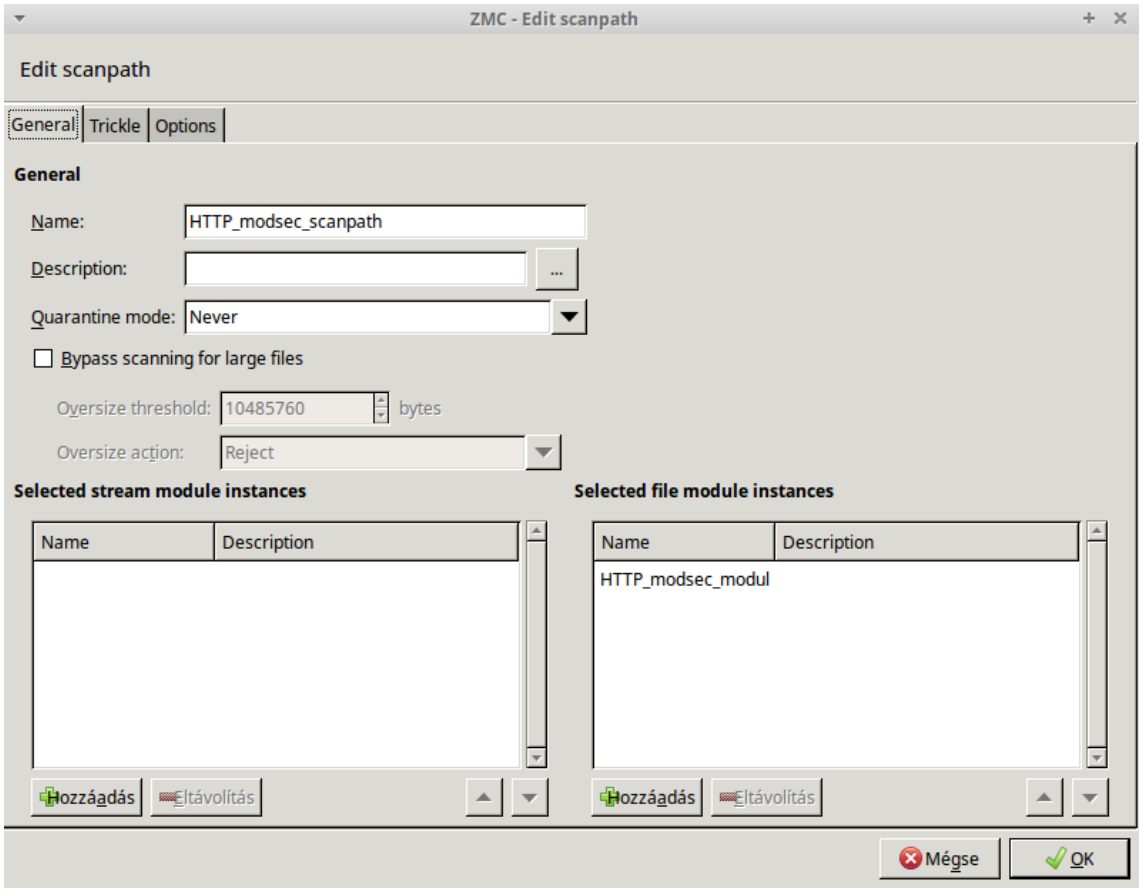
2. Aktiválja a *Zorp Management Server (ZMS)* konfigurációban a *ModSecurity* plugint:
   Új *Komponens → Texteditor → ModSecurity with OWASP CRS template*

   Később ezt a konfigurációt fogjuk a tűzfalra szabni.

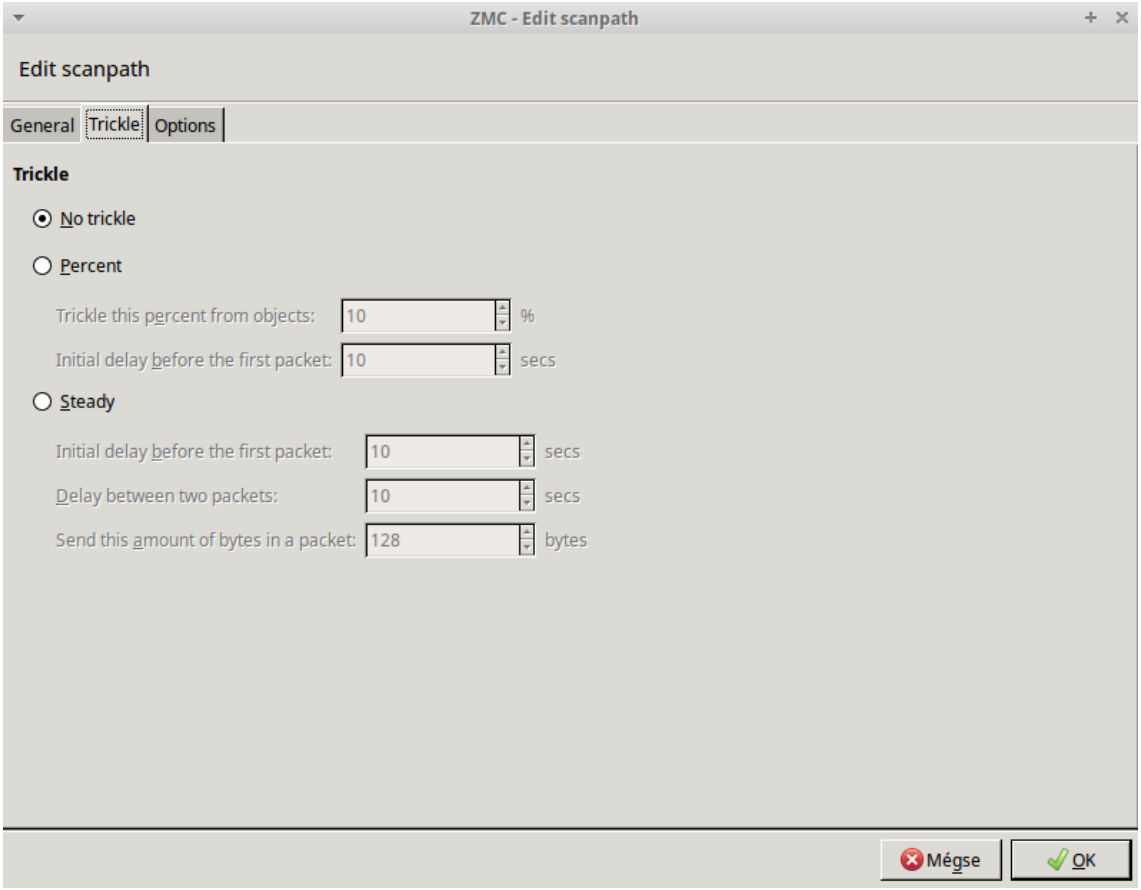
3. Konfigurálja a *ZMC*-t az alábbiak szerint. Figyeljen, hogy a konfigurációs fájl útvonala megfelelő legyen:



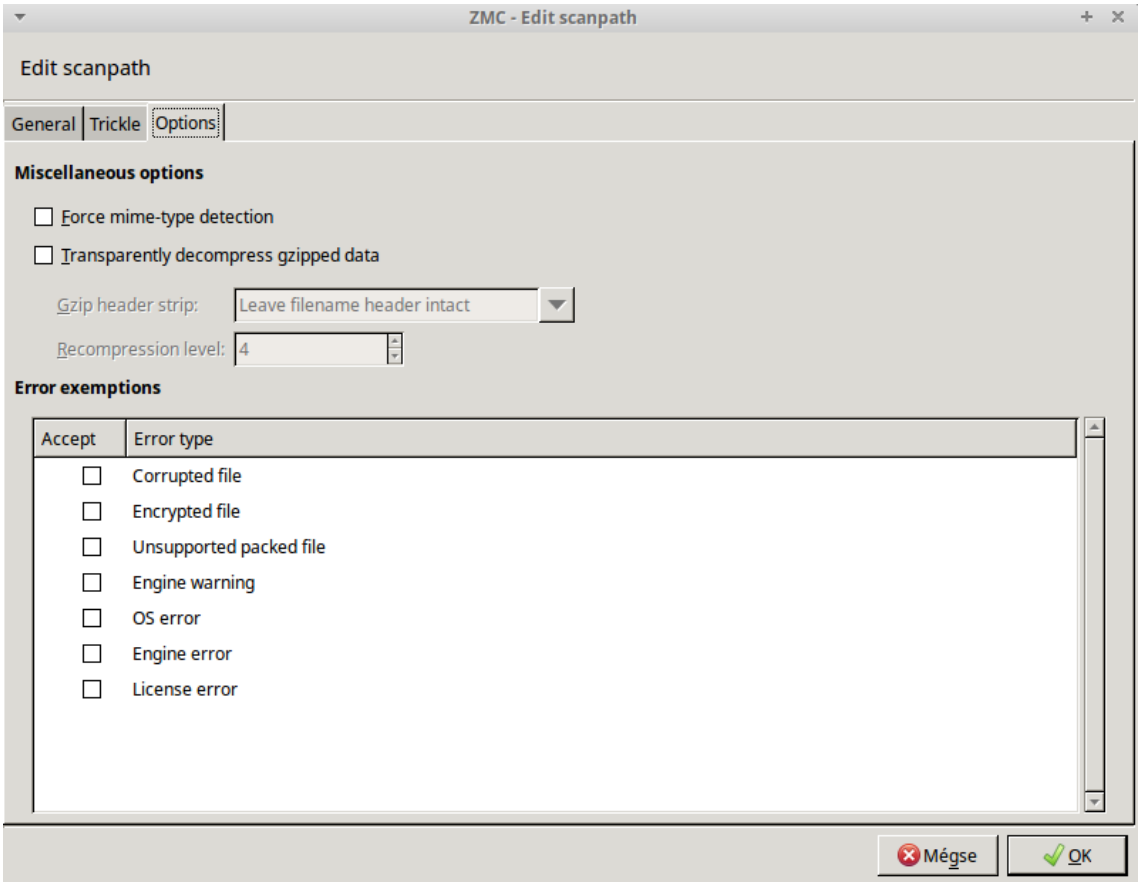

*1. ábra - ZMC module instance szerkesztése*



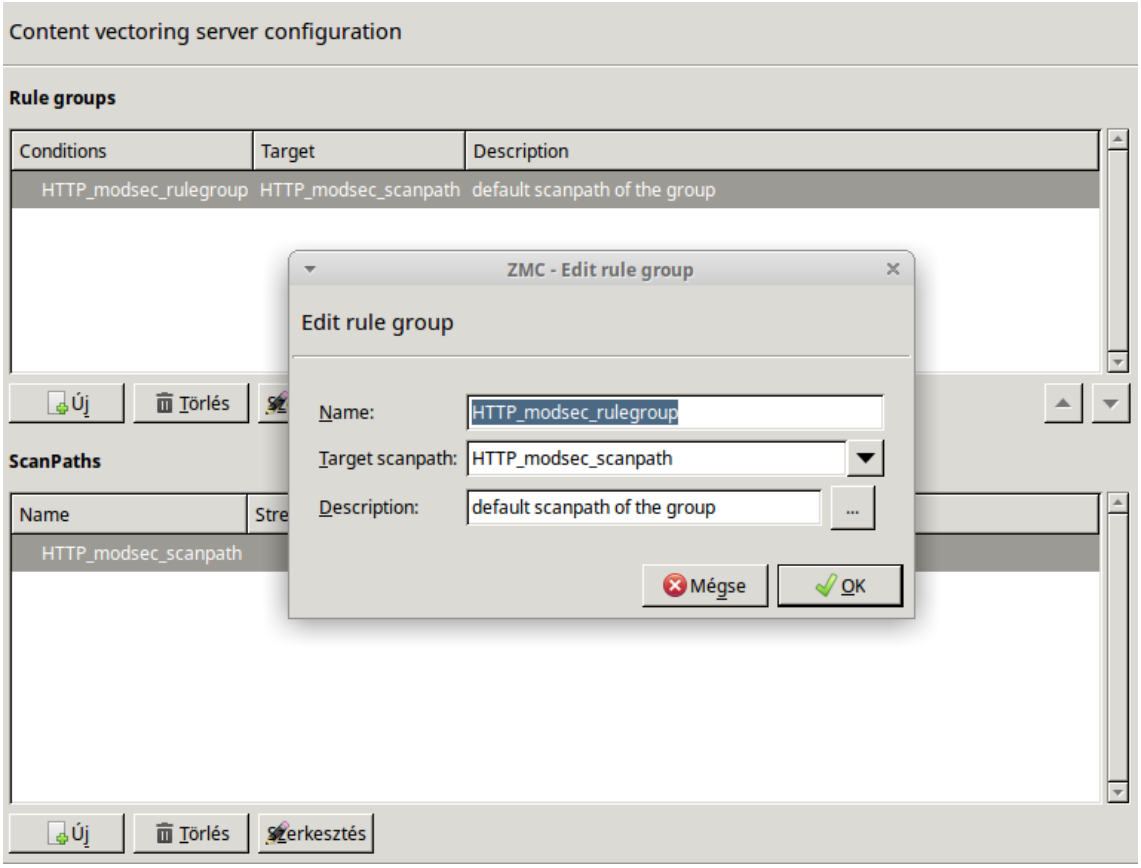

*2. ábra - Scanpath szerkesztése - General*




*3. ábra - Scanpath szerkesztése - Trickle*

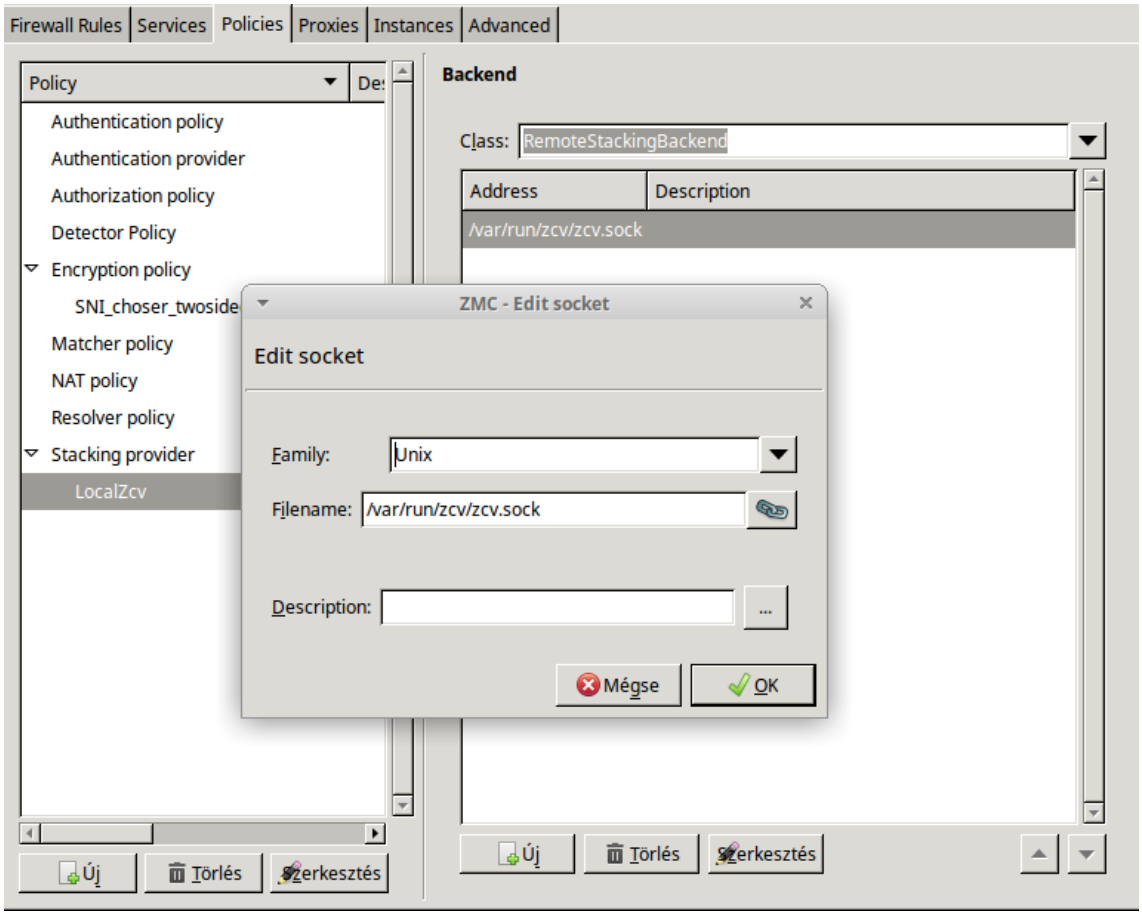



*4. ábra - Scanpath szerkesztése - Options*



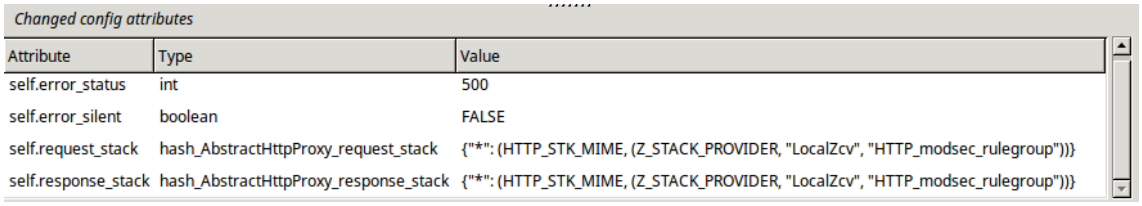

*5. ábra - Rule group szerkesztése - Options*

Ezt a *ZCV* scanpath útvonalat a *Zorp Gateway* felé mint „stacking provider” szabályt (policyt) kell felmutatni.




*6. ábra - Socket szerkesztése - Options*

Majd ezt a megfelelő HTTP proxyba kell beágyazni.




*7. ábra - Változó attribútumok*

Így az összes HTTP kérés és válasz a *ZCV ModSecurity* útvonalán fog áthaladni.

Ezután a rendszer működése elviekben már tesztelhető, de szabályok híján minden forgalmat át fog engedni.

4. Szerezze be a szabályokat. Erre több lehetőség van. A legegyszerűbb megoldás erre az Ubuntu 18.04 LTS -t használni:

```
sudo apt install modsecurity-crs
```

Ez egy viszonylag régi szabálystruktúrát telepít, de feltelepíti a következő fájlt, amire szükségünk lesz, hogy a többnyelvű forgalmat is eredményesen elemezhesse a modul:

```
/usr/lib/modsecurity/unicode.mapping
```

5. Ezt másolja át az etc/zcv könyvtár alá:

```
sudo cp /usr/lib/modsecurity/unicode.mapping /etc/zcv/
```

6. Szerezzen be egy friss szabályrendszert a következő paranccsal:

```
# cd /etc/zcv/etc/
        zcv# sudo git clone https://github.com/coreruleset/coreruleset
```

7. Ellenőrizze az eredményt:

```
/etc/zcv# cd owasp-modsecurity-crs
/etc/zcv/owasp-modsecurity-crs# git pull

Already up to date.
```

A két utolsó parancsból egy cron-jobot generálva az adatbázisunkat frissen tarthatjuk.

8. Alakítsa a *ModSecurity texteditor plugint* a következőképpen:
Az oldal alján lévő hasonló sorok elé szúrjuk be a következő sorokat:

```
Include /etc/zcv/owasp-modsecurity-crs/crs-setup.conf.example
Include /etc/zcv/owasp-modsecurity-crs/rules/*.conf
```

A fájl közepén található:

```
SecDebugLog /var/log/modsecurity/debug.log
```

9. Állítsa a *SecDebugLogLevel 3* sorokat teszteléshez *SecDebugLogLevel 7* -re, majd töltse fel és indítsa újra a *ModSecurity*t.

## 3.1. Ellenőrzés

Amennyiben minden eddigi beállítás megfelelő, a rendeltetésszerű webes forgalmunk továbbra is zavartalanul fog működni, de egy, a szabályokra pozitív teszttel érdemes ezt ellenőrizni:

```
https://védett.szerverünk.saját.címe/aphpfilethatdonotexist.php?something=../../etc
```

- Ellenőrzés a *Zorp Content Vectoring System* logokban:

```
core.info(4): (zcv/scan:1): Sending verdict; verdict='reject',
description='This content is rejected by
       local policy settings', details='Web application firewall detected
 rule violation'
```

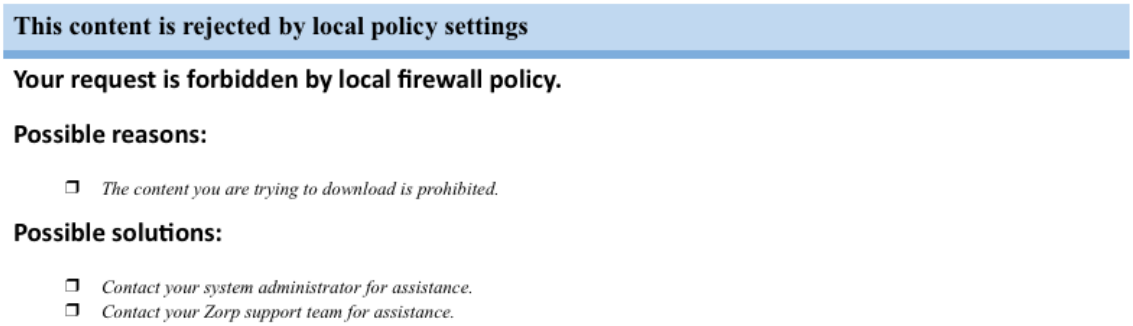
- Ellenőrzése a `/var/log/modsecurity/debug.log-ban`:

```
[157623444919.158715]
[https://védett.szerverünk.saját.címe/aphpfilethatdonotexist.php?something=../../etc]
 [4]

Running (disruptive)  action: deny.
```

A fentiekből is látható, hogy a forgalmat a *Zorp Gateway* nem engedte át.

A böngészőben a kék *Zorp* hibaoldal fogadja a felhasználót:




*8. ábra - A hibaoldal*

Ezt később tetszés szerint kikapcsolhatjuk a HttpProxy attribútum használatával:

```
„self.error_silent=TRUE”
```

Személyre is szabhatjuk a hibás fájlokat, ha azokat a `/usr/share/zorp/http` könyvtárból egy másik könyvtárba másoljuk (mivel itt a *Zorp* frissítés a változtatásainkat felülírja). Átírjuk őket, majd a „self.error_files_directory=” HttpProxy attribútumot megfelelően kitöltjük.

## 4. Konklúzió

Bár a megoldási lehetőségek rugalmassága miatt a modul integrálása nem teljesen magától értetődő (texteditor plugin, git clone), és a szabály adatbázis verziójának váltásakor a konfiguráció módosítást igényelhet, a megoldás egy erőteljes és automatikus védelmi réteget képez, melynek alkalmazása webszerverek védelménél erősen javasolt.