Spam előszűrés *Zorp Gateway*-el

2022. július 28.

Az alábbi esettanulmány a *The Spamhaus Project* által publikus szolgáltatásként nyújtott IP reputációs, DNS protokollal lekérdezhető Real-time Blocklist (RB) spam adatbázis használatát ismerteti a *Zorp proxyban*.

Tartalom

1. A probléma bemutatása

A levélforgalom nagy része spam, melynek szűrése nagyon leterheli a meglévő antispam rendszereket. Ha az ismert lánclevél küldő forrásokat már a kapcsolat elején blokkoljuk (prefiltering), a levél tartalmának analizálását végző modulnak már nem kell ezek feldolgozásával tovább terhelni a rendszert.

2. A megoldás bemutatása

A *Zorp Gateway* SMTP (Simple Mail Transfer Protocol) proxyjába könnyen beilleszthető egy olyan kódrészlet, ami DNS feloldással lekérdezi a zen.spamhaus.org spam adatbázisát. Kis forgalmú cégeknél saját célra integrálva szabadon használható az ingyenes szolgáltatás. Termékbe integrálva, nagyvállalatok részére kb. 2 USD/fő/év a költsége. Ezért a termék részeként nem szállítjuk, de ha a végfelhasználó kéri, a spam szűrő megoldása elé tudunk illeszteni egy ezt használó megoldást, amit integrálni tudunk a *Zorp* proxyba.

3. Technikai megvalósítás

A *Spamhaus* egy felhő szolgáltatás, amely DNS kérésekkel operál, ezért hatékony és sávszélesség takarékos. A fizetős verzió az erre használt DNS zónának saját szerverre történő zóna transzferét teszi lehetővé.

3.1. Példák IP cím lekérdezésére

Nem SPAM forrású IP címek lekérdezése:

```
~$ host mail.balasys.hu
mail.balasys.hu has address 185.199.30.237
~$ host 237.30.199.185.zen.spamhaus.org
Host 237.30.199.185.zen.spamhaus.org not found: 3(NXDOMAIN)
```

SPAM forrású IP címek lekérdezése:

```
~$ host 212.109.237.14.zen.spamhaus.org
212.109.237.14.zen.spamhaus.org has address 127.0.0.11
~$ host 212.109.237.114.zen.spamhaus.org
212.109.237.114.zen.spamhaus.org has address 127.0.0.11
212.109.237.114.zen.spamhaus.org has address 127.0.0.3
212.109.237.114.zen.spamhaus.org has address 127.0.0.4
```

A válasz alapján az IP címet több kategória is tartalmazza.

3.2. Az IP címeket tartalmazó kategóriák feloldása

DNSBL	Lekérdezendő domain	Visszatérési érték	Tartalom
SBL	sbl.spamhaus.org	127.0.0.2-3,9	Statikus, ellenőrzött SPAM források, cégek
XBL	xbl.spamhaus.org	127.0.0.4-7	Jellemzően feltört, vírusos gépek, botnetek, trójaiak kategóriája
PBL	pbl.spamhaus.org	127.0.0.10-11	Publikus IP címek, ahonnan nem ajánlott autentikáció nélkül levelet fogadni (tipikusan dinamikus ISP előfizetői allokációk)
ZEN	zen.spamhaus.org	127.0.0.2-11	Kombinált adatbázis (ajánlott) tartalmazza az SBL, XBL és PBL kategóriákat is.

1. ábra - IP címek feloldása

Megjegyzés
SBL: Spamhouse Block List

XBL: Exploits Block List

> PBL: Policy Block List
>
> ZEN: Zen

Számunkra az SBL és XBL osztályok az érdekesek. A biztosan SPAM küldőket letiltjuk.

Az erre használható *Zorp*-6-os proxy osztály:

```
class RBLSpamFilterSmtpProxy(SmtpProxy):

    def config(self):

        super(RBLSpamFilterSmtpProxy, self).config()

        self.request["MAIL"] = (SMTP_REQ_POLICY, self.checkRBL)


    def checkRBL(self, cmd, param):

        proxyLog(self, CORE_POLICY, 5, "Starting RBL checking.")

        l = string.split(self.session.client_address.ip_s, ".")

        l.reverse()

        lookup_host = string.join(l, ".") + "." + self.rbl_domain

        proxyLog(self, CORE_POLICY, 5, "Looking up RBL; query_string='%s'",
lookup_host)

        try:

           addr = socket.gethostbyname(lookup_host)

        except socket.error:

            addr = None

     if addr:

         if '127.0.0.2' in addr or '127.0.0.3' in addr or '127.0.0.9' in addr:

            proxyLog(self, CORE_POLICY, 2, "Address in Direct RBL, rejecting;
ip='%s', rbl='%s', response='%s'",
                  (self.session.client_address.ip_s, self.rbl_domain, addr))

             return SMTP_REQ_ABORT

           elif '127.0.0.4' in addr or '127.0.0.5' in addr or '127.0.0.6' in addr
 or '127.0.0.7' in addr:

          proxyLog(self, CORE_POLICY, 2, "Address in XBL RBL, rejecting; ip='%s',
 rbl='%s', response='%s'",
```

```
            (self.session.client_address.ip_s, self.rbl_domain, addr))

            return SMTP_REQ_ABORT

        else:

            return SMTP_REQ_ACCEPT


"BlackList"""

MatcherPolicy(name="EmailBlackList",
matcher=RegexpFileMatcher(match_fname="/etc/zorp/email-blacklist",
 ignore_fname="/etc/zorp/email-blacklist.ignore"))

MatcherPolicy(name="InterSMTPRecipientMatcher",
matcher=RegexpFileMatcher(match_fname="/etc/zorp/email-recipient",
 ignore_fname="/etc/zorp/email-recipient.ignore"))



class InterSmtpProxy(RBLSpamFilterSmtpProxy):

    def config(self):

        RBLSpamFilterSmtpProxy.config(self)

        self.request_stack["*"]=(SMTP_STK_MIME,
         (Z_STACK_PROVIDER, "LocalZCV", "InterSMTPScanning"))

        self.relay_domains=("saját domain helye.hu", )

        self.sender_matcher="EmailBlackList"

        self.recipient_matcher="InterSMTPRecipientMatcher"

        self.rbl_domain="zen.spamhaus.org"

        self.max_request_length=1024

        self.unconnected_response_code=451

        self.require_crlf=FALSE

        self.relay_check=TRUE

        self.error_soft=TRUE
```

A proxyt érdemes az SMTP autentikációt ellenőrző proxyval kombinálni, amennyiben a belső szerver ezt támogatja.

```
class AuthRelaySmtpProxy(SmtpProxy):

    def config(self):

        SmtpProxy.config(self)

        self.response["AUTH", "235"] = (SMTP_RSP_POLICY, self.authsucc)



    def authsucc(self, cmd, cmd_param, rsp, rsp_param):

        self.relay_check = FALSE

        log(None, CORE_POLICY, 3, "Relay-check disabled after successful auth;
         rsp='%s'; rsp_param='%s'", (rsp,rsp_param,))

        return SMTP_RSP_ACCEPT
```

4. Konklúzió

A fenti proxyval az ismert spam források kiszűrhetők, így csak a spamek fennmaradó részével kell a belső, *Zorp Content Vectoring System*-alapú spam filternek (SpamAssasin) vagy a belső szerveren futó egyéb antispam alkalmazásnak megküzdenie. Kisebb ügyfeleknél önmagában elegendő a levélforgalom kordában tartására ez a megoldás, nagyvállalati szinten terheléscsökkentő spam előszűrőként alkalmazható. Különösebb karbantartást nem igényel.