SPF, MTA-k és SRS

Az előző cikkben áttekintettük, hogy DNS segítségével hogyan jelölhetjük meg eredetiként kimenő elektronikus leveleinket. Most eljött az ideje annak, hogy a bejövő levelek ellenőrzéséről is gondoskodjunk, és megvédjük felhasználóinkat a hamisított, kéretlen levelektől és a férgektől.

A Sender Policy Framework (SPF, küldő házirend-keretrendszer) a válaszútvonal hamisítása ellen segít védekezni – amit általában férgek, vírusok és levélszemét terjesztők alkalmaznak. Az SPF életre hívása két szakaszból áll. Először a rendszergazdák SPF-bejegyzéseket tesznek közzé a DNS-ben. Ezek a bejegyzések az egyes tartományok által a kimenő levelek kezelésére használt kiszolgálókat adják meg. Az SPFre képes MTA-k (***mail transport agent***, levéltovábbító ügynök) később ellenőrzik a bejegyzéseket. Ha egy levél nem az SPF-ben megadott kiszolgálóról érkezik, akkor bátran hamisnak nyilváníthatjuk.
A továbbiakban – kapcsolódva előző írásomhoz – felvázolom, hogyan ruházhatjuk fel SPF képességekkel a levélkiszolgálónkat. Szó lesz arról is, hogy az elektronikus leveleket továbbító, vagy weben előállító szolgáltatások a küldő módosításával hogyan működtethetők tovább az SPF bevezetése után is.

Az MTA bővítése SPF-képességekkel

A linuxos világ legfontosabb levéltovábbító ügynökei (***MTA***) a Sendmail, a Postfix, a Qmail és az Exim. Noha a legtöbb levélszemétszűrő megoldást kínáló cég már megoldotta az SPF támogatását (vagy legalábbis tervezi), az MTA-k esetében ez a feladat ránk vár. Az SPF-MTA együttműködést kétféle módon valósíthatjuk meg.
Aki szereti maga lefordítani a programokat, az az SPF letöltési oldalán kezdjen, itt ugyanis mindenki megtalálja a saját MTA-jához készült SPF modult és a hozzá tartozó telepítési útmutatót. Aki inkább csomagkezelővel telepíti a programokat, az nagy valószínűséggel talál olyan előre fordított MTA-változatot, amely eleve támogatja az SPF használatát. A legtöbb beépülő modulnak szüksége van a ***Mail::SPF::Query Perl*** könyvtárra.
A könyvtár a ***CPAN***-ról telepíthető a legkönnyebben, de csomag formájában is megpróbálhatjuk előkeresni. Lényegében egy egyszerű programot biztosít az SPF-lekérdezések parancssorból való futtatására. Egy egyszerű démont is tartalmaz, amely UNIX-tartományon vagy ***inet*** foglalaton keresztül kezeli az SPF-kéréseket.
A beépülő modulok nagy része alapesetben az SPF alapú ellenőrzésen megbukó üzenetek elutasítására szólítja fel az MTA-t, a többihez pedig egy `Received-SPF` fejlécet fűz. Ha kissé mértéktartóbbak akarunk lenni, akkor elutasítás helyett a `Received-SPF: fail` sorral is bővíthetjük a fejlécet. Ezt a lehetőséget a beépülő modulok leírása ismerteti bővebben.

Sendmail

A Sendmail beépülő modulok fogadására szolgáló felületét Milternek nevezzük. (Lásd az internetes forrásokat.) Az újabb Sendmail-változatok alapesetben is támogatják a Milter használatát. A Sendmail foglalat alapú felületen keresztül tartja a kapcsolatot a Milterrel. Értesíti azt a befelé irányuló SMTP-tranzakciókról, a Milter pedig megmondja a Sendmailnek, hogy mit kell tennie. A Milter démonként fut, indítása is külön történik. Az SPF weboldalon két Milter érhető el, egy Perl és egy C alapú. A Perl alapú változat kifinomultabb, ha viszont gyorsabb működést szeretnénk, akkor a C alapú változatot válasszuk. A Milter és a Sendmail együttműködéséhez néhány sorral bővíteni kell a sendmail.mc fájlt, újra kell fordítani a ***sendmail.cf***-et, majd újra kell indítani a Sendmailt. Ha inkább nem akarjuk használni a Miltert, a libspf-hez tartozik egy olyan folt is, ami lehetővé teszi az SPF közvetlen beépítését a Sendmailbe.

Postfix

A Postfix 2.1 házirend démon felülettel rendelkezik. Ennek működése nagyon hasonló a Milteréhez: a Postfix csatlakozik a démonhoz, átadja a szükséges adatokat, majd a démon egy művelettel válaszol a Postfixnek. Ha a 2.0-s sorozat újabb, fejlesztői kiadását futtatjuk, akkor ellenőrizzük, hogy 2.0.18-20040122-es vagy újabb változattal rendelkezünk-e.
A házirend démonok beállításai a ***main.cf*** és a ***master.cf*** fájlban szerepelnek. Kezelésükről a Postfix gondoskodik, indításukat és leállításukat szükség szerint elvégzi, így ezzel nem kell foglalkoznunk. A Postfix házirend démon Perlben készült, működéséhez szükség van a normál ***Mail::SPF::Query*** könyvtárra.

Exim

Az Exim 4 újdonsága az Access Control Lists (ACLs), ami egy sokoldalú, kisméretű programozási mininyelv levélszemét szűrésére és egyéb házirend jellegű döntések leírásához. Az SPF Exim alatti használatához szükséges ACL kód nagyjá-

ból 12 sort tesz ki. Telepíteni kell a ***Mail::SPF::Query*** könyvtárat és futtatni ennek SPF démonját, amely megadott foglalaton hallgatózik. Az SPF ACL csatlakozik az ***spfd***-hez és átadja neki az ügyfél IP-címét, a HELO kapcsolót és a MAIL FROM küldő címet. Ezután kap valamilyen SPF-eredményt, választ az SMTP-kiszolgálóra vonatkozóan, valamint egy Received-SPF fejlécsort. Az ***spfd***-t külön kell indítani.

Qmail

A Qmail nem rendelkezik olyan beépülő modul felülettel, mint a többi MTA. Létezik viszont olyan SPF-folt, amely az SPF-et közvetlenül a Qmailbe építi. Emellett sok Qmail-használó ***qpsmtpd*** segítségével szűri leveleit. Aki ezt a megoldást választotta, az beépülő modulként könnyen be tudja kapcsolni az SPF-et.
A ***C SPF*** könyvtár készítésében James Couzens játssza a főszerepet. A ***libspf***-hez Qmailhez és egyéb MTA-khoz készült folt egyaránt tartozik.

A beépülő modul kipróbálása

A beépülő modul telepítése és bekapcsolása után két ellenőrzést kell végrehajtani. Az első és legfontosabb annak ellenőrzése, hogy a tiszta levelek átjutnak-e. Ha nem, akkor lehetséges, hogy nem fut valamelyik szükséges program, ekkor végezzünk ismételt ellenőrzést. Ha továbbra is gondjaink vannak, állítsuk vissza a régi rendszert, és jelezzük a hibát az spf-help levelezési listán.
A második próba alkalmával a hamisított levelek elutasítását kell ellenőrizni. Ha kézzel lépünk be az SMTP-kiszolgálóra, akkor ***MAIL FROM:linuxjournal-test@altavista.com*** származással hozzunk létre egy levelet. Az ***altavista.com*** tartományt levelezésre nem használják, ezért ilyen küldőre minden esetben FAIL jelzést kell kapnunk. Többen kérdezték, hogy a próbaüzenetekben szerepeljen-e a test/teszt szó. Ezt kockázatos megtenni, mert ha megbízható ügyfelet vélnek felismerni, saját MTA-nk és SPF-ünk hamis levelet is átengedhet. Telneten keresztül tehát ne lépjünk be a helyi gépre, inkább használjuk gépünk valódi állomásnevét, és ha mód van rá, a kapcsolatot külső állomásról kezdeményezzük. Ha 550-es választ és az ➲ http:\\spf.pobox.com/why.html oldalra hivatkozó hibaüzenetet kapunk, a rendszer működik. Ha másodlagos MX-et használunk, akkor utasítsuk SPF-ügyfelünket, hogy ne tagadja meg ennek leveleit. Minderről részletesen a beépülő modul telepítési útmutatójából tájékozódhatunk.

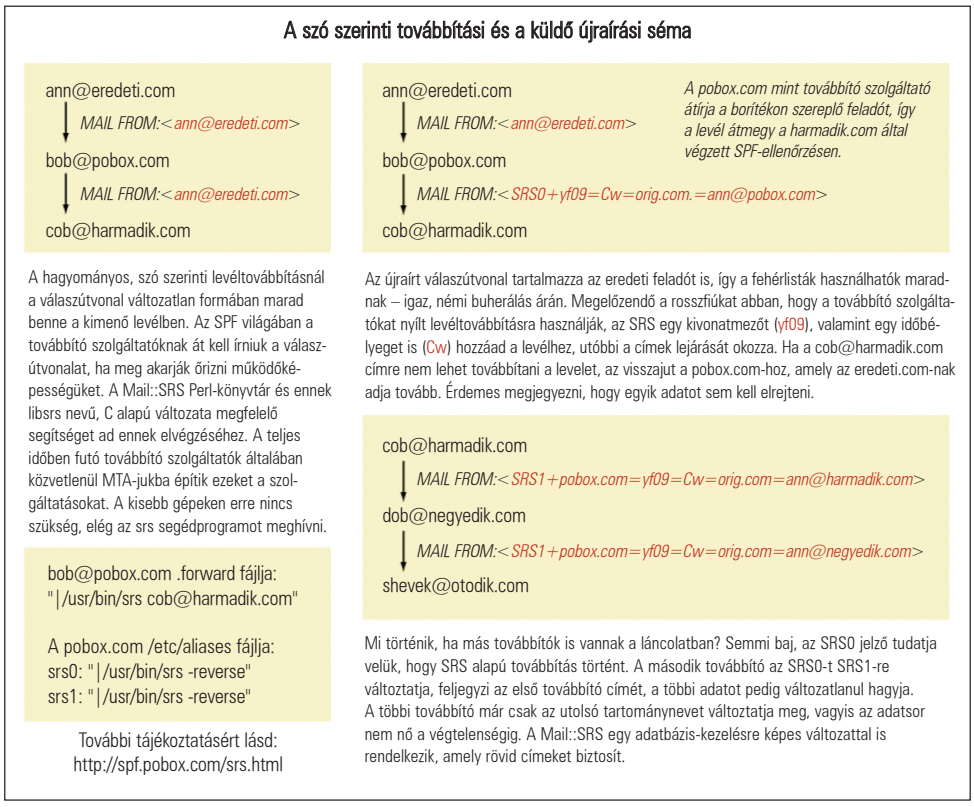
Received-SPF: a kódok jelentése

Mint azt látni fogjuk, leveleink immár egy Received-SPF fejlécet is tartalmaznak, amelyben különféle eredménykódokat találhatunk:

- `NONE`: A tartományhoz nem tettek közzé SPF-bejegyzéseket. Az MTA-nak a szokásos módon kell folytatnia munkáját.
- `PASS`: A levél nem hamis, de az sem biztos, hogy valódi. Ne feledjük, a levélszemetek küldői is közzétehetnek SPF-bejegyzéseket. A tartományt valamilyen fehérlista alapján ellenőrizni kell. Ha a küldő egy általunk megbízhatónak vélt fehérlistán szerepel, akkor a további ellenőrzéseket nyugodtan elhagyhatjuk.
- `FAIL`: A levél hamis, nyugodtan eldobhatjuk. Csekély valószínűséggel előfordulhat, hogy a levél tiszta feladótól érkezett, ám annak beállításait hibásan adták meg. Ha ez a helyzet, akkor a küldő fél hibaüzenetet kap, amelyben levélküldő ügynökének (Mail User Agent, MUA) SMTP AUTH használatára való beállítására szólítjuk fel. Az SPF tervezési elve szerint jobb egy szívélyes hibaüzenet küldése mellett hibát elkövetni, mint mély hallgatással egy levélszemetes ládába hajítani az üzeneteket.
- `SOFTFAIL`: Lehetséges, hogy az üzenet hamis, de a tartomány internetszolgáltatója már megkezdte a felhasználók rendszereinek átállítását SMTP AUTH használatára, tehát előfordulhat, hogy a levél tiszta. Az üzenetet célszerű fogadni, de érdemes további ellenőrzéseknek alávetni.
- `NEUTRAL`: A tartományban megkezdték az SPF bevezetését, alapértelmezett válaszuk `?all`. Szeretnék azt a látszatot kelteni, mintha a válasz NONE lenne, amíg a SOFTFAIL és a FAIL alapértelmezett válaszokat be nem vezetik. A nagyméretű, több millió ügyfelet kiszolgáló internetszolgáltatók lassan követik a dolgokat – ez van, nem az ő hibájuk.
- `ERROR`: Alkalmi hiba lépett fel a DNS-keresésnél. Normál esetben ilyenkor saját MTA-nknak 450-es kódú ideiglenes hibát kell jeleznie.
- `UNKNOWN`: Állandó jellegű hiba miatt az SPF-keresés félbemaradt. Lehetséges, hogy gépelési hiba van a bejegyzésben, esetleg egy másik tartományra mutat, amelyhez viszont nem tartozik SPF-bejegyzés.

Az SPF bevezetésének ára

Az elmúlt tíz évben az elektronikus levelezés egyre nagyobb szerephez jutott. Hogy pontosan mennyire függünk tőle, arról csak akkor kapunk képet, amikor egy-egy féreg elárasztja a hálózatot. Az elemzők ilyenkor rutinszerűen közlik, hány milliárd dolláros kárt okoznak a gazdaságnak a kéretlen levelek és a vírusok. Az SPF sikere is bizonyítja, az emberek nagyon várják már a változásokat.
Minden változásnak megvan azonban az ára. Ha volna valami fájdalommentes megoldás a levélszemét gondjára, már nyilván mindenki bevezette volna. A levélszemét elleni küzdelem régóta húzódik, mert a legnagyobb szakértők képtelenek megegyezni a szükséges ellenlépésekben – szerencsére a vita lezárulni látszik. Minden levélszemét elleni megoldásban közös és alapvető elem a küldő fél hitelesítése. Erre már számos modellt dolgoztak ki, ám ezek közül az SPF „megnevezett küldő” szemléletű megoldását a legkönnyebb megvalósítani. A jövő kétségkívül a titkosításé, de arra még várni kell. Az elsősegélyként alkalmazható SPF előnyei azonnal megmutatkoznak, és megvalósításával sem kell késlekednünk. De mi az SPF használatának ára? Minden megnevezett küldő alapú sémánál két dolog módosulásával kell számolni. Az első az, hogy az SPF ellehetetleníti a szó szerinti levéltovábbítást. (*1. ábra*) Vannak olyan szolgáltatások, amelyeket az emberek általában azért vesznek igénybe, mert változatlan e-mail címet biztosítanak. Ezek a UNIX ***.forward*** és a ***/etc/aliases*** fájloknál megismert módon továbbítják a leveleket. Amikor egy levél elhagyja a kiszolgálót, a borítékján szereplő válaszútvonal változatlan marad. Az SPF használatakor azonban a továbbított levelek hamisnak tűnnek. A megoldás az, hogy a továbbító szolgál-



1. ábra SPF használatakor az elektronikus levelek hagyományos továbbítása nem lehetséges

leveleket eldobják. Az újabb, haladó szellemiségű webhelyek, mint például az ***Orkut***, valami ilyet tesznek. Ha viszont a levelek fontosak, és elküldésükre a webhelyre szabályosan bejelentkezett felhasználók nevében kerül sor, valamint a webhely üzemeltetője korábban ellenőrizte a felhasználók e-mail címét, akkor a webhely SRS-t is alkalmazhat – vagyis, ha beágyazzák a felhasználó válaszcímét, akkor a visszapattanó leveleket is könnyedén el tudják juttatni rá. Jogos a kérdés: mi lesz az átállás ideje alatt? Nem lesznek leállások, amíg a továbbító szolgáltatók nagy nehezen megvalósítják az SRS támogatását? Mi lesz azokkal a szolgáltatókkal, akik túl lassan lépnek, vagy képtelenek alkalmazkodni? Van itt egy apró titok. Nagyjából sejteni lehet, kik lógnak ki a sorból. Van egy fehérlistát, amelyen a jó szándékú hamisítók szerepelnek. A listán szerepel például a ***pobox.com***, az ***acm.org***, az eBay és számos „elküldöm ezt a cikket e-mailben” jellegű szolgáltatást kínáló hírmagazin. Az eddig említett SPF-ügyfelek mindegyike képes kezelni a fehérlistát. A fehérlista formájában tehát minden ismert SPF-ügyfélnél megvan az utolsó esély a végleges elutasítás előtt. Ha az anyukánk küld nekünk egy levelet az AOL-os hozzáféréséről az ***acm.org***-os címünkre, akkor az SPF-ügyfelünk fogadni fogja a levelet, noha műszakilag hamis lesz. (Ha a levelet út közben olyan rendszer – például egy barátunk linuxos kiszolgálója – is továbbítja, amely nem szerepel a fehérlistán, akkor hozzá kell adnunk saját MTA-nk fehérlistájához ezt a gépet.) Amikor az ***acm.org*** megvalósítja az SRS támogatását, a kérdés megoldódik. Az SPF-et bírálók ellenérvként a levéltovábbítás ellehetetlenülését szokták felhozni. Az SPF közösség nem hagyta szó nélkül a kifogásokat, mindent megtett az átállás megkönnyítésének érdekében. Két megoldást is kidolgoztak, egy rövid és egy hosszú távút. Jó ha tudjuk, minden változás fájdalmas. Az SPF-re való áttérés is gondokkal jár, ám a betegségtől gyakran csak a kellemetlen injekció segítségével szabadulhatunk meg. Márpedig az elektronikus levelezés nagyon beteg. Vannak, akik szerint a levélszemét meg fogja ölni, de én ezt nem hiszem. Szerintem az SPF biztos kézzel fogja a gyógyulás útjára segíteni.

tatók újraírják a levelek válaszútvonalát. Ugyancsak így kell tenniük a leveleket a .forward és a ***/etc/aliases*** fájlok alapján továbbküldő szervezeteknek. Ez a megoldást SRS-nek (sender rewriting scheme, küldő újraírási séma) nevezzük. Az eredeti küldő címét egy újraírt, SPF-megfelelő válaszcímbe ágyazza be. Ha egy üzenet visszapattan, akkor hozzánk érkezik be, ilyenkor ki kell hámoznunk a címet, majd továbbítani a levelet az eredeti feladónak. A továbbító szolgáltatóknak akkor is meg kell tenniük mindezt, ha nem használnak SPF-et, az internetszolgáltatók ugyanis már végeznek SPF jellegű ellenőrzéseket. Az SPF csupán egy szabványos eljárást biztosít arra, amit a legtöbb helyen már most is megtesznek. Ahogy a felelősséggel vezetett szolgáltatók néhány éve megszüntették a nyílt levélküldési lehetőségeket, úgy a következő hónapok során az SPF-megfelelő továbbítást is be fogják vezetni. A ➲ http:\\www.pobox.com már alkalmazza az SRS-t, és hamarosan más továbbító szolgáltatók is követni fogják a példáját. A jó hír az, hogy az SPF-et fejlesztő közösség az MTA-khoz tartozó SRS kódot is elkészítette. Ezek a foltok ugyanonnan érhetők el, mint az SPF foltok. Az SRS elterjedése csupán idő kérdése. Az SPF azonban a webről küldött leveleket is megállíthatja. Az üdvözlőlapok küldésére használható oldalak és az „elküldöm ezt a cikket egy barátomnak” jellegű szolgáltatások általában nemcsak a From: fejlécben de, borítékon is a szolgáltatást igénybe vevő személy címét tüntetik fel. Az SPF az ilyen leveleket nem képes megkülönböztetni a hamisítottaktól.
A gondra kétféle megoldás létezik. Az első, hogy úgy döntenek, az ilyen levelek nem túl fontosak, válaszútvonalként a ***senki@példa.com***-ot adják meg, aztán a visszapattanó

Linux Journal 2003. november, 115. szám

Meng Weng Wong