Az SMTP AUTH beállítása

IP cím ellenőrzés helyett hitelesítsük Postfix kiszolgálónk felhasználóit név és jelszó alapján – avagy ami nem állandó, az fix, hogy megváltozik.

Egyszer volt, hol nem volt, volt egyszer egy rendszergazda. A szemfüles olvasó bizonyára felfedezte azt, hogy az előző cikkem is ugyanezen felütésszerű mondattal kezdődött. Az egybeesés nem véletlen. Hősünk ebben a mesében sem lesz más, mint a mérnöki tudományok teljes fegyvertárát zsonglőrként alkalmazó rendszergazda, aki alig várja, hogy a felhasználók igényeinek kielégítése után következhessen a megérdemelt pihenés.

Eme jubileuminak mondható második epizód sem különbözik az elsőtől. A rendszergazda vígan tengeti életét, mígnem a felhasználók világvége hangulatot idéző sikoltásai nyomán szembekerül a problémával. Első benyomásra a problémának hét feje van és lángok csapnak fel szörnyűséges torkából, de közelebbről megvizsgálva kiderül, hogy csak egy pici gyíkról volt szó. A szükséges intézkedések nyomán hősünk végleges megoldást talál, és láthatjuk a könnyű nyáresti szellő borzolta hajkorona sziluettjét a lemenő nap utolsó sugaraiban.

Ne szaladjunk azonban előre! Rendszergazdánk munkahelyén a levelező kiszolgálót helyi hálózaton keresztül érik el a munkaállomások. Természetesen ugyanennek a számítógépnek van egy lába az Internet felé is, valamint egy *DNS*-ben jegyzett *MX* rekordja. Ez egy igen kellemes kialakítás, hiszen a kötelező biztonság mellett egyszerűen beállítható és karbantartható. Ne felejtsük el, hogy ha lehet választani, hősünk mindig az egyszerűbb megoldás mellett dönt.

A levélküldő kiszolgáló egy előfordított *Debian* csomagból telepített *Postfix*. Miután a cég összes munkaállomása a helyi hálózaton van, kézenfekvő beállításnak tűnt a ***levéltovábbítás (smtp relay)*** engedélyezése a teljes belső hálózatra. Miután történetünk rendszergazdája felvette az alábbi sort a */etc/postfix/main.cf* fő konfigurációs állományba, az e-mail küldés már működött is. Csupán némi finomhangolás maradt hátra, melyet itt most nem részleteznék.

```
mynetworks = 127.0.0.0/8, 192.168.0.0/24
```

Telt, múlt az idő, és a cég vezetősége egy új iroda létrehozását tűzte ki célul. Nem tervezték azonban külön *SMTP* kiszolgáló felállítását a létesítményben. Feltételezték, hogy egy közönséges *ADSL* kapcsolat előfizetésével a levelezés kérdésére megadták a választ. Sebtében kiadták a parancsot hősünknek, nevezetesen „legyen e-mail”. Bár a rendszergazdák isteni származása megkérdőjelezhetetlen tény, és így bizonyításra nem szorul, sajnos ezúttal nem élhetek a szent könyvekből ismert pátoszos fordulattal, miszerint „és lőn”.

A gondot az jelentette, hogy az *ADSL* előfizetés dinamikusan változó *IP* címre szólt. Mikor rendszergazdánk felvetette ezt a problémát a cég vezetőinek, arra kellett rádöbbennie, hogy minden jó szándék mellett a pánikhangulatnál többet nem tud elérni náluk. Így számba vette a szóba jöhető ötleteket és elkezdte latolgatni a várható előnyöket és hátrányokat. Négy gondolatfoszlány suhant át az agyán.

Az első, és egyben magától értetődő ötlet a fentebb említett `mynetworks` sor bővítése. Mivel a *Postfix* alapvetően *IP* cím alapján azonosít, elképzelhető, hogy ha egy kellően tág tartományban engedélyezett a levéltovábbítás, akkor ezzel hősünk átvágta a gordiuszi csomót. A kellően tág tartomány jelen esetben azt jelentené, hogy fel kell venni azt a teljes IP cím tartományt, amelyből a távoli iroda ***internet-szolgáltatója (ISP, Internet Service Provider)*** *IP* címet oszthat.

Égbekiáltó gaztett lenne a fentebb vázolt kósza gondolat kivitelezése. Ezáltal az összes, ugyanahhoz a szolgáltatóhoz tartozó vadidegen előfizetőnek engedélyezve volna a levélküldés. Ez nem pusztán biztonsági rés, de könnyen meg is utáltathatja vele magát a meggondolatlan adminisztrátor. A levélszemetet ontó kiszolgálót nem igazán szeretik az Internet harcedzett használói. Mi több, egy ilyen merénylet elkövetése után a kiszolgáló teljesen jogosan bekerülhet a ***Nyitott Átjárók Adatbázisába (Open Relay Database, http://www.ordb.org/)***, ami által számos e-mail kiszolgáló eleve el fogja utasítani az összes, tőle érkező levelet.

Második lehetőségként felmerülhet a dinamikusan osztott *IP* kézzel történő felvétele a fenti sorba. Persze ami kézi szerkesztéssel kivitelezhető, az megoldható szkripttel is. Még azonban így is rá kell bírni a távoli iroda átjáróját arra, hogy valahogyan tudassa az új címet, ezután újra kell tölteni a *Postfix* konfigurációt. Ez az elképzelhető legkörülményesebb, és túl sok helyen támadható. Néha be kell látni, hogy az egyszerűbb lehet bonyolultabb is.

Az első két gyenge próbálkozásra fátylat borítva hősünknek eszébe ötlött, hogy látott már olyan levelező programot, ami támogatta a ***POP-before-SMTP*** nevű eljárást. Ez a körültáncolt problémára egy olyan csellel nyújt megoldást, hogy a levelező program küldés előtt feljelentkezik a ***POP3*** kiszolgálóra. Miután ott hitelesítette magát, és az ***SMTP*** kiszolgáló erről tudomást szerzett, a felhasználó szabadon küldheti leveleit. Ezt azonban nem minden levelező ügyfél támogatja.

A múlt megnyugtató homályába veszett gondolatkísérletek után rendszergazdánk rátalált a legelfogadhatóbb megoldásra. Az eljárás neve ***SMTP AUTH***, és arról szól, hogy minden ügyfél az IP cím helyett egy név és jelszó páros segítségével nyer hitelesítést. A levelező programokban csak egy ezt az információt kell megadni, a kiszolgáló helyes beállítása mellett innentől zavartalanul folyhat az e-mail küldés.

Ennek a módszernek megvan az a határtalan szépsége, hogy hosszú távú megoldást biztosít. Egy újabb telephely létrehozása után minden további beállítás nélkül használható a levelező kiszolgáló. Mindössze a megfelelő felhasználókat kell létrehozni. Természetesen ezeknek nem kell rendszerfelhasználóknak lenniük, de ez egy másik mese. Rendszergazdánk megtalálta tehát a megoldást. Ezek után lássuk, mi hogyan kivitelezhetjük az ötletet.

A ***SASL*** a ***Simple Authentication and Security Layer*** rövidítése, és a 2222-es számú ***RFC*** taglalja részletesen. Érdemes a ***Cyrus-SASL*** nevű megvalósítás használatában elmélyedni, ha másért nem, azért, mert temérdek dokumentáció áll rendelkezésre az Interneten a szoftver használatához. Számos hitelesítési forrást kezel, sajnos azonban ***SQL*** adatbázisból, vagy ***LDAP*** kiszolgálótól egyelőre nem tudja közvetlenül lekérdezni a szükséges információkat. Ilyen jellegű igény esetén a forráskód foltozása az egyetlen út.

Telepíteni kell tehát egy ***Cyrus-SASL*** nevű szoftvert, valamint biztosítani kell, hogy a ***Postfix*** képes legyen a használatára. ***Debian*** alatt ez egyszerűen a ***postfix-tls*** csomag kiválasztásával elérhető. Mivel ez a csomag függ a megfelelő ***SASL*** csomagoktól, és fel is ajánl számos olyat, ami hasznos lehet a későbbiekben, érdemes az összes szintű függőséget kielégíteni. Miután szélsebesen feltelepítettünk mindent, következhet a beállítás.

Az első és legfontosabb teendő a meglévő ***main.cf*** állomány biztonsági másolatának elkészítése. Miután meggyőződtünk róla, hogy minden, amit ezután teszünk, visszafordítható folyamatot jelent, ragadjunk klaviatúrát és egy sokat próbált szövegszerkesztőnk segítségével nyissuk meg a konfigurációs állományt. Az első, amit a ***Postfix*** tudtára kell hozni, az az hogy használnia kell a ***SASL***-t.

```
smtpd_sasl_auth_enable = yes
```

Ezzel a sorral mellesleg remekül lehet ellenőrizni a ***postfix-tls*** csomag jelenlétét, illetve forráskódból történő telepítés esetén a megfelelő fordítás előtti beállítások helyességét. Ha a ***Postfix*** hibaüzenetet dob a fenti sorra hivatkozva, biztosak lehetünk benne, hogy hiányzik valamilyen összetevő a rendszerből. Következzen ezután egy biztonsági beállítás.

```
smtpd_sasl_security_options = noanonymous
```

Ezáltal kizárható a névtelen bejelentkezés lehetősége, mivel az ***SMTP*** kiszolgáló fel sem fogja ajánlani az ügyfélnek a hitelesítés ezen módját. A hitelesítési mód a sima szöveges bejelentkezéstől kezdve a ***Kerberos***-ig sokféle lehet, beleértve az imént kizárt módot is. Egy bizonyos hitelesítési forrás használatakor, melyre később még visszatérünk, szükséges a következő.

```
smtpd_sasl_local_domain = $myhostname
```

Ez egyfajta tartománynevet állít be, de hangsúlyozom, hogy alább még szó esik erről. Fontos továbbá a régebbi levelező programok támogatása is.

```
broken_sasl_auth_clients = yes
```

A ***Microsoft Outlook Express 4***, illetve a ***Microsoft Exchange 5.0*** két olyan meglehetősen régi levelező, amellyel az ***SMTP AUTH*** kommunikáció a szigorú szabványok megtartása mellett nem működik. A fenti sor ezen a gondon segít, és egyes szabványok enyhébb figyelembevételével lehetővé teszi azoknak az ügyfeleknek is a hitelesítést, melyek már kifejezetten korosnak mondhatók. Végezetül határozzuk meg, hogy a ***SASL*** hitelesített felhasználók küldhetnek a kiszolgálón keresztül levelet.

```
smtpd_recipient_restrictions =
    permit_sasl_authenticated,
    permit_mynetworks,
    check_relay_domains
```

Látható, hogy a kiszolgáló a `mynetworks` sorban szereplő ***IP*** címekről továbbra is fogadja a levelet, egy másik lehetőség a hitelesítés. A fenti változtatások eszközölése után újra be kell olvastatni a ***Postfix*** beállítási állományait. Ezt az alábbi paranccsal érhetjük el.

```
# /etc/init.d/postfix reload
```

A hitelesítés már működik is! Csak a hitelesítés forrása nincs meghatározva, ez viszont már csak ujjgyakorlat. A szigorúan hitelesítéssel kapcsolatos beállítások a ***/etc/postfix/sasl/smtpd.conf*** nevű állományban találhatók. Könnyen elképzelhető, hogy sok rendszeren ez az állomány nem létezik, ekkor kézzel kell létrehozni. Az is lehet, hogy a ***/usr/lib/sasl*** könyvtárban kell keresni a nevezett fájlt. Ez a helyzet többek között akkor, ha forráskódból történik a telepítés.

Az állomány legfontosabb paramétere a `pwcheck_method`. Valójában nincs is olyan sok beállítási lehetőség, de erre nem is volna szükség. Ezzel az egy paraméterrel a hitelesítés forrása könnyűszerrel állítható. A következő sorral meghatározzuk, hogy `sasldb`-t használunk erre a célra.

```
pwcheck_method: sasldb
```

Ez egy igen tipikus felhasználás. Nincs szükség az azonosításhoz külön démonra, ugyanis egy Berkeley adatbázisból nyeri a felhasználónevet, illetve a jelszót.

Az adatbázis a */etc/sasldb* néven található. Ebben a név és jelszó mellett még egy ***tartománynév (realm)*** is szerepel. Ennek az az oka, hogy ha egy levelező kiszolgáló több tartományért is felel, fontos lehet megkülönböztetni az egyik tartományban szereplő felhasználót a másik tartománybeli azonos nevű felhasználótól. Fontos, hogy a sasldb használatakor a hitelesítés csak akkor sikeres, ha a *Postfix main.cf* állományának `smtpd_sasl_local_domain` paraméterében ugyanazt a tartomány szerepel, mint ami az adott felhasználónévhez tartozik ebben az adatbázisban.
Már csak egy dolog maradt hátra. Hozzunk létre egy felhasználót, aki jogosult használni az *SMTP* kiszolgálót, *IP* címétől függetlenül. `sasldb` használatakor ez a következő paranccsal tehető meg.

```
# saslpasswd -c -u mail.vallalat.hu geza
```

Ezzel létrehoztunk egy */etc/sasldb* nevű állományt, ha az még nem létezett, és szerepel benne az új bejegyzés. A felhasználó neve `geza`, a `mail.vallalat.hu` tartomány tagja (realm), jelszava pedig a `saslpasswd` által bekért szó.
A `sasldb` egy *Berkeley* adatbázis, ezért ne számítsunk arra, hogy közönséges szövegmegjelenítővel emészthető formában látjuk a tartalmát, viszont a `sasldblistusers` segítségével remekül lehet böngészni is.

```
# sasldblistusers
```

Felhívnám a figyelmet arra, hogy ha a *Postfix* gyökérkönyvtárat vált indulás után (*chroot*), ennyivel még nem fogja megtalálni */etc/sasldb* néven az adatbázist. Ez a helyzet az előfordított Debian csomag esetén is. Ez esetben az állományt másoljuk át a *Postfix* új gyökerébe.

```
# cp /etc/sasldb /var/spool/postfix/etc/
➥ sasldb
```

Elkészültünk. Természetesen a hitelesítési forrás megváltoztatásával elérhető, hogy ne legyen szükség külön felhasználói névre és jelszóra az *SMTP*-hez. Például *Cyrus IMAP* kiszolgáló esetén hitelesítési forrásként a `pwcheck`-et megadva az *IMAP*-es név és jelszó páros is minden további nélkül használható. További lehetőség a `shadow` érték, amivel a rendszeradatbázist foghatjuk munkára. Ez azonban komolyan ellenjavallt, amellett, hogy gyökérváltás után el sem érhető.

Sok sikert a beállításokhoz és biztonságos levelezést mindenkinek!

Fülöp Balázs (admin@guardware.com)
21 éves, imádja a Túró Rudit, a Debian Linuxot és a teheneket. Kedvenc írója Slawomir Mrožek. Leginkább a számítógépes hálózatok biztonsága érdekli. A BME VIK műszaki informatikus szak hallgatója.