

SASL SMTP autentikacija u Postfixu



U tipičnom slučaju kojeg možemo naći na institucijama članicama CARNeta mail poslužitelj se nalazi na lokaciji gdje se nalazi većina zaposlenika, a institucija ima eventualno još jednu lokaciju ili nekoliko njih. Kako bi korisnici mogli slati mail preko tog poslužitelja, Postfix je potrebno konfigurirati tako da zaprima mailove (radi *relay*) iz "domaćih" mrežnih segmenata i šalje ih na odredište. Ovo je lako napraviti, jer samo treba u varijablu `$mynetworks` upisati novi segment i restartati Postfix.

Problem nastaje kada korisnici žele slati mailove od kuće, ili sa službenog puta. U tom slučaju nemamo izbora nego dodati sve segmente određenog ISP-a kako bi korisnik mogao slati mail iz mreže baš tog ISP-a. Kasnije, javit će se drugi korisnik koji rabi drugi ISP, pa moramo dodati i te segmente i tako unedogled. Jasno je da dodavanje drugih mrežnih segmenata otvara Vaš mail poslužitelj eventualnim spammerima iz Hrvatske (ili korisnicima koji ni ne znaju da su im računala zaražena kakvim crvom). Ukoliko korisnik putuje u inozemstvo, praktički je nemoguće saznati koji će segment korisnik rabiti za spajanje.

Postoji nekoliko načina da riješimo ovaj problem:

Možemo uputiti korisnike da na putu ili od kuće rabe webmail na vašim stranicama ili pak preko središnjeg servisa <http://webmail.carnet.hr> [1]. U ovom slučaju se može pojaviti problem, ako korisnici rabe zastarjeli POP3 protokol. Tada neće imati sinkronizirano stanje na vlastitom računalu sa stanjem na poslužitelju (npr. neće imati poslane mailove u Outlooku ili Thunderbirdu, nego će ti mailovi biti samo na poslužitelju).

Najbolje je rješenje rabiti SMTP autentikaciju preko SASL daemona. Na ovaj način moguće je slati mailove preko poslužitelja na vašoj ustanovi preko bilo koje mreže. Jedini uvjet je da se korisnik prethodno "predstavi" sustavu, dakle upiše svoje podatke (username i password) u svoj mail klijent.

Svi mail klijenti podržavaju ovu mogućnost autentikacije, pa jedino ostaje da korisnicima podesite mail klijente ili im date upute kako da to sami učine. Jednom podešeni klijenti mogu nastaviti raditi i "kod kuće" i unutar lokalne mreže, samo će se u logovima vidjeti novi unosi poput "sasl_username" i "sasl_method":

```
May 31 12:43:48 server postfix/smtpd[3298]: connect from
pc-racunalo.domena.hr[161.53.XX.YYY]
May 31 12:43:59 server postfix/smtpd[3298]: 38BE9135957: client=
pc-racunalo.domena.hr[161.53.XX.YYY], sasl_method=PLAIN,
sasl_username=korisnik@domena.hr
```

Nikako **nemojte uključivati** opcije "Use Secure Authentication", "Secure Password Authentication (SPA)" i slično. Radi se o Microsoftovim metodama autentikacije i na Postfixu neće raditi. Sva potrebna podešavanja na Postfixu su već napravljena, ukoliko imate CARNet paket postfix-cn. U `/etc/postfix/main.cf` bi trebale biti uključene ove opcije:

```
smtpd_sasl_auth_enable = yes
smtpd_sasl_security_options = noanonymous
smtpd_sasl_local_domain = $myhostname
broken_sasl_auth_clients = yes
```

```
smtpd_recipient_restrictions = permit_mynetworks,  
                             permit_sasl_authenticated, ...
```

Jedino, možete provjeriti je li pokrenut saslauthd proces:

```
# ps -ef |grep saslauthd  
root      3030      1  0 Apr08 ?          00:00:00 /usr/sbin/saslauthd  
-a pam -c -m /var/run/saslauthd -n 5  
root      3036     3030  0 Apr08 ?          00:00:00 /usr/sbin/saslauthd  
-a pam -c -m /var/run/saslauthd -n 5  
...
```

Dakle, sve je u redu, SASL daemoni su pokrenuti. Ukoliko nisu, provjerite zašto po uputama u članku <http://sistemac.carnet.hr/node/122> [2].

Navest ćemo podešenja za dva najpopularnija mail klijenta:

Mozilla Thunderbird:

Tools -> Account Settings -> Outgoing Server -> Edit -> <pod "Security and Authentication" kliknuti na "Use Name and Password" -> <popuniti podatke>

Settings

Description: SMTP sa autentikacijom

Server Name: server.domena.hr

Port: 25 Default: 25

Security and Authentication

☒ Use name and password

User Name: korisnik

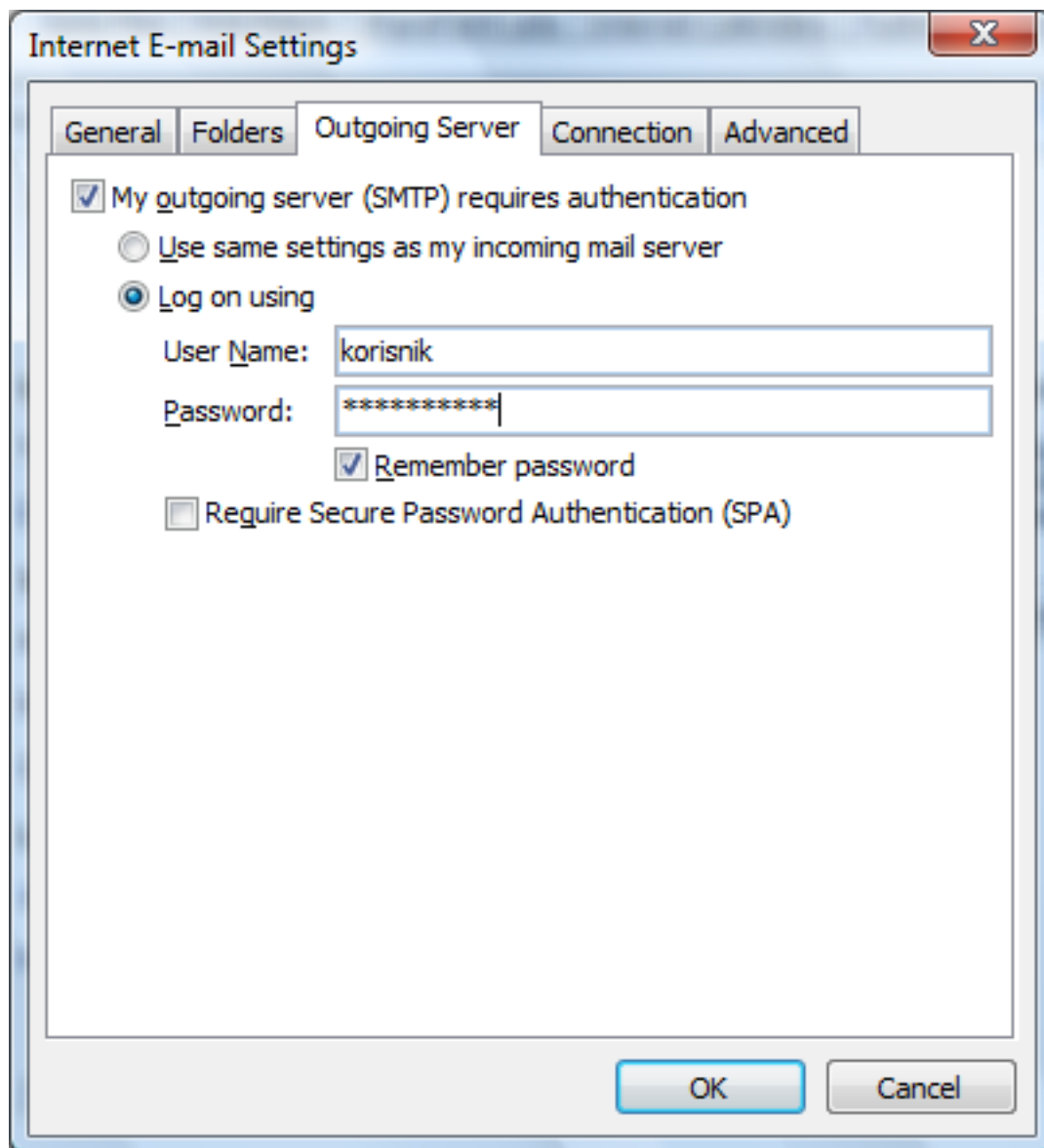
☐ Use secure authentication

Connection security: None

OK Cancel

Microsoft Outlook:

Tools -> Account Settings -> <dvoklik na profil>
-> More Settings -> Outgoing Server -> <upišite podatke> -> <isključiti SPA>



Za druge klijente je postupak, pretpostavljamo, vrlo sličan, pa ne bi trebao biti problem i njih podesiti.

Više o načinu rada SASL autentikacije, možete pročitati u članku "[SASL - Simple Authentication and Security Layer](#) [3]"

- [Logirajte](#) [4] se za dodavanje komentara

pon, 2010-05-31 13:24 - Željko Boroš**Vote:** 5

Vaša ocjena: Nema Average: 5 (2 votes)

story_tag: [SASL](#) [5]
[postfix](#) [6]
[SMTP AUTH](#) [7]

[SPA](#) [8]

[saslauthd](#) [9]

Source URL: <https://sysportal.carnet.hr/node/747>

Links

[1] <http://webmail.carnet.hr>

[2] <https://sysportal.carnet.hr/node/122>

[3] <https://sysportal.carnet.hr/node/764>

[4] <https://sysportal.carnet.hr/sysportallogin>

[5] <https://sysportal.carnet.hr/taxonomy/term/143>

[6] <https://sysportal.carnet.hr/taxonomy/term/122>

[7] <https://sysportal.carnet.hr/taxonomy/term/144>

[8] <https://sysportal.carnet.hr/taxonomy/term/145>

[9] <https://sysportal.carnet.hr/taxonomy/term/146>