راه‌اندازی و پیکربندی امن پروتکل SSL/TLS بر روی سرویس‌دهنده پست الکترونیک Postfix 3.0

شماره مستند APA-AMIRKABIR-13950703-1
تاریخ نگارش ..... ۳ مهر ۱۳۹۵
شماره نگارش ۱/۰
نگارش ..... آپای امیرکبیر
طبقه‌بندی ..... عادی

فهرست مطالب

۱ مقدمه

شرکت‌ها و سازمان‌های کوچک عمدتاً از شرکت‌های سرویس‌دهنده Hosting برای پست الکترونیک خود استفاده می‌کنند اما شرکت‌های متوسط و بزرگ به دلیل مسائل امنیتی و حساسیت سرویس پست الکترونیک برای آنان، ناچار به استفاده از یک Mail Server اختصاصی در محل خود هستند.

برای تأمین محرمانگی و جامعیت داده‌های مبادله شده می‌توان از پروتکل‌های استانداردی که بدین منظور طراحی شده استفاده کرد. در حال حاضر مهم‌ترین پروتکل رمزنگاری که در سطح اینترنت برای رمزنگاری داده‌های لایه کاربرد و تأمین امنیت ارتباطات استفاده می‌شود، پروتکل SSL/TLS است. در این گزارش، راه‌اندازی و پیکربندی امن پروتکل SSL/TLS بر روی سرویس‌دهنده پست الکترونیک Postfix 3.0 بیان شده است.

۲ فعال‌سازی ارتباطات SSL/TLS

برای پیکربندی SSL/TLS و استفاده از این پروتکل ابتدا باید گواهی‌نامه دیجیتال مربوطه را از مراکز صدور گواهی (CA)[۱] معتبر دریافت کرد (یا گواهی خود-امضا[۲] را تولید کرد). گرفتن گواهی دارای مراحلی است که برای اطلاعات بیشتر در این زمینه می‌توانید به گزارش ارائه شده توسط پژوهشکده آپای دانشگاه صنعتی امیرکبیر که در آدرس زیر قرار دارد مراجعه کنید:

http://apa.aut.ac.ir/?p=971

در ادامه قصد داریم تا فایل پیکربندی Postfix را که در مسیر زیر قرار دارد را به منظور استفاده از SSL/TLS و پیکربندی امن آن، ویرایش کنیم:

```
/etc/postfix/main.cf
```

توجه: قبل از انجام تغییرات روی این فایل، یک نسخه پشتیبان از آن تهیه کنید.

برای استفاده از ارتباطات SSL/TLS باید مسیرهای مربوط به فایل کلید خصوصی و همین‌طور گواهی اصلی و گواهی‌های میانی را به پارامترهای مربوطه بدهیم که در زیر نشان داده شده است.

```
smtp_use_tls = yes
# smtpd_tls_auth_only = yes <-- Optional
smtpd_tls_cert_file = /some/path/yourdomain.crt
smtpd_tls_key_file = /some/path/yourdomain.key
smtpd_tls_CAfile = /some/path/ca.txt (bundle file)
```

فایل گواهی (yourdomain.crt)، یک موجودیت عمومی (غیر محرمانه) است ولی فایل کلید (yourdomain.key) به صورت محرمانه نگهداری می‌شود. زمانی که از یک مراکز صدور گواهی میانی، گواهی دریافت کنید، آن CA، زنجیره گواهی‌های میانی خود را در قالب یک بسته[۳] در اختیار شما قرار می‌دهد که در خط چهارم از جدول بالا، پارامتر مربوطه مقدار دهی شده است. البته می‌توان فایل گواهی اصلی و میانی را در یک فایل با دستور زیر ترکیب کرد:

```
cat yourdomain.crt ca.txt > server.crt
```

و با ترکیب این دو گواهی، مقدار دهی به پارامترها به صورت زیر تغییر می‌کند:

```
smtp_use_tls = yes
# smtpd_tls_auth_only = yes <-- Optional
smtpd_tls_cert_file = /some/path/server.crt
smtpd_tls_key_file = /some/path/yourdomain.key
```

توجه کنید که خط دوم اختیاری است و در صورتی که تمایل دارید تا تمام سرویس‌گیرنده‌ها فقط از طریق ارتباطات رمز شده به شما متصل شوند، این گزینه را فعال کنید. با فعال سازی این مورد، درخواست‌هایی که از TLS استفاده نمی‌کنند، رد می‌شوند.

بعد از انجام این مراحل، فایل main.cf را ذخیره کرده و سرور Postfix را با دستور زیر راه‌اندازی مجدد کنید:

---

۱ Certificate Authority

۲ Self-signed certificate

۳ Bundle

مرکز پژوهشی آپا (آگاهی‌رسانی، پشتیبانی، امداد برای آسیب‌پذیری‌ها و حوادث امنیتی سایبری)
تهران - بالاتر از چهارراه ولیعصر - نبش کوچه بالاور – ساختمان معاونت پژوهشی دانشگاه صنعتی امیرکبیر - طبقه سوم
کد پستی: ۱۵۹۱۶۳۴۳۱۱ تلفکس: ۶۶۴۶۰۳۰۸ Web: https://apa.aut.ac.ir - Email: autcert@aut.ac.ir

```
sudo postfix reload
```

۳ پیکربندی امن پروتکل SSL/TLS

در این بخش چگونگی پیکربندی امن پروتکل SSL/TLS را در سرویس‌دهنده پست الکترونیک Postfix 3.0 بیان می‌کنیم. مواردی همچون استثنا کردن برخی الگوریتم‌های رمزنگاری به منظور کاهش حملاتی شبیه به FREAK، CRIME و LogJAM، غیرفعال سازی نسخه‌های ناامن SSL و برقرار کردن رمزنگاری‌های قوی که از Forward Secrecy (FS) پشتیبانی می‌کنند را در این بخش بیان می‌کنیم.

برای بررسی وضعیت امنیتی پروتکل SSL/TLS سرویس‌دهنده خود، می‌توانید به ابزاری که بدین منظور توسط پژوهشکده آپای دانشگاه صنعتی امیرکبیر طراحی شده و در آدرس زیر قرار دارد، مراجعه کنید.

https://sslcheck.certcc.ir

۳–۱ غیرفعال کردن SSLv2 و SSLv3

SSLv2 و SSLv3 ناامن هستند و باید غیرفعال شوند. برای غیرفعال سازی آنها، خط مربوطه از فایل مخصوص پیکربندی را به صورت زیر ویرایش می‌کنیم:

```
# Disable SSLv2 and SSLv3 leaving TLSv1, TLSv1.1 and TLSv1.2 enabled.
smtpd_tls_mandatory_protocols = !SSLv2, !SSLv3
smtpd_tls_protocols = !SSLv2 !SSLv3
```

۳–۲ غیرفعال سازی الگوریتم‌های رمزنگاری ضعیف

Forward Secrecy اطمینان می‌دهد که صحت[۱] یک کلید جلسه[۲] حتی وقتی که کلیدهای زیادی مورد مخاطره قرار گرفتند، حفظ می‌شود. FS کامل[۳] این مورد را با استخراج یک کلید جدید برای هر جلسه، به انجام می‌رساند. این بدان معناست که زمانی که کلید خصوصی به مخاطره افتاد، نمی‌تواند برای رمزگشایی ترافیک SSL مورد استفاده قرار گیرد.

پیشنهاد می‌شود دستور زیر را برای استفاده از الگوریتم‌های رمزنگاری قوی و غیرفعال سازی رمزنگاری‌های ضعیف در فایل پیکربندی وارد کنید.

```
# Configure the allowed cipher list
smtpd_tls_mandatory_ciphers=high
tls_high_cipherlist=EDH+CAMELLIA:EDH+aRSA:EECDH+aRSA+AESGCM:EECDH+aRSA+
SHA384:EECDH+aRSA+SHA256:EECDH:+CAMELLIA256:+AES256:+CAMELLIA128:+AES12
8:+SSLv3:!aNULL:!eNULL:!LOW:!3DES:!MD5:!EXP:!PSK:!DSS:!RC4:!SEED:!ECDSA
:CAMELLIA256-SHA:AES256-SHA:CAMELLIA128-SHA:AES128-SHA
```

۱ Integrity

۲ Session Key

۳ Perfect Forward Secrecy

مرکز پژوهشی آپا (آگاهی‌رسانی، پشتیبانی، امداد برای آسیب‌پذیری‌ها و حوادث امنیتی سایبری)
تهران - بالاتر از چهارراه ولیعصر - نبش کوچه بالاور – ساختمان معاونت پژوهشی دانشگاه صنعتی امیرکبیر - طبقه سوم
کد پستی: ۱۵۹۱۶۳۴۳۱۱ تلفکس: ۶۶۴۶۰۳۰۸ Web: https://apa.aut.ac.ir - Email: autcert@aut.ac.ir

۳–۳ امن سازی پارامترهای دیفی هلمن

ما نیاز داریم تا یک پارامتر دیفی هلمن قوی را تولید کنیم، که می‌توانیم با دستور زیر این کار را انجام دهیم:

```
openssl gendh -out /etc/postfix/dh_1024.pem -2 1024
```

و سپس باید به Postfix بگوییم که از این پارامترها برای تغییر کلید دیفی هلمن[۱] استفاده کند و برای این کار، باید خط زیر را در فایل پیکربندی اضافه کنیم:

```
#the dh params
smtpd_tls_dh1024_param_file = /etc/postfix/dh_1024.pem
```

۴–۳ غیرفعال سازی SSL Compression

با وجود SSL Compression، حمله CRIME ممکن است انجام شود و ما باید آن را غیرفعال کنیم. دستور زیر، SSL compression را غیرفعال می‌کند.

```
# Disable SSL compression
tls_ssl_options = NO_COMPRESSION
```

۱ DHE key-exchange

مرکز پژوهشی آپا (آگاهی‌رسانی، پشتیبانی، امداد برای آسیب‌پذیری‌ها و حوادث امنیتی سایبری)
تهران - بالاتر از چهارراه ولیعصر - نبش کوچه بالاور – ساختمان معاونت پژوهشی دانشگاه صنعتی امیرکبیر - طبقه سوم
کد پستی: ۱۵۹۱۶۳۴۳۱۱ تلفکس: ۶۶۴۶۰۳۰۸ Web: https://apa.aut.ac.ir - Email: autcert@aut.ac.ir

۴ منابع

1 https://www.instantssl.com/ssl-certificate-support/email-certificate/postfix.html

2 http://www.postfix.org/TLS_README.html

3 https://blog.tinned-software.net/harden-the-ssl-configuration-of-your-mailserver/

4 https://zmap.io/sslv3/servers.html#postfix

5 ftp://ftp.cs.uu.nl/mirror/postfix/FORWARD_SECRECY.html

مرکز پژوهشی آپا (آگاهی‌رسانی، پشتیبانی، امداد برای آسیب‌پذیری‌ها و حوادث امنیتی سایبری)
تهران - بالاتر از چهارراه ولیعصر - نبش کوچه بالاور – ساختمان معاونت پژوهشی دانشگاه صنعتی امیرکبیر - طبقه سوم
کد پستی: ۱۵۹۱۶۳۴۳۱۱ تلفکس: ۶۶۴۶۰۳۰۸ Web: https://apa.aut.ac.ir - Email: autcert@aut.ac.ir