SSL

SSL - Background

SSL (Secure Sockets Layer) adalah protokol keamanan yang dikembangkan oleh Netscape pada pertengahan 1990-an untuk mengenkripsi komunikasi antara server web dan browser pengguna. Tujuan utama SSL adalah melindungi data sensitif seperti informasi login, data pribadi, dan transaksi keuangan dari penyadapan dan manipulasi selama transmisi.

Latar Belakang :

1. Pengembangan : SSL pertama kali diperkenalkan oleh Netscape pada tahun 1994 sebagai SSL 2.0. Versi ini memiliki beberapa kelemahan keamanan, sehingga SSL 3.0 dirilis pada tahun 1996 dengan perbaikan signifikan.

2. Penggantian oleh TLS : Pada tahun 1999, SSL berevolusi menjadi TLS (Transport Layer Security), yang merupakan versi yang lebih aman dan efisien. Meski begitu, istilah SSL masih umum digunakan untuk merujuk pada teknologi enkripsi ini.

3. Fungsi : SSL/TLS menggunakan enkripsi untuk melindungi data selama transmisi, memastikan integritas data, dan menyediakan autentikasi antara server dan klien. Ini memungkinkan pengguna untuk berkomunikasi secara aman melalui internet.

SSL telah menjadi standar dalam melindungi komunikasi online, terutama dalam e-commerce, layanan perbankan, dan situs web yang memerlukan data pribadi.

SSL - Create CSR

Generate CSR file dengan Langkah-langkah sebagai berikut :

1. Buat private key dengan command sebagai berikut :

```
openssl genrsa -des3 -out ilusidigital.key 2048
```

2. Buat file CSR menggunakan key yang sudah dibuat dengan perintah sebagai berikut :

```
openssl req -new -key ilusidigital.key -out ilusidigital.csr
```

3. Isi parameter sesuai identitas perusahaan :

```
Country Name (2 letter code) [GB]:ID
State or Province Name (full name) [Berkshire]:Bogor
Locality Name (eg, city) [Newbury]:Bogor Utara
Organization Name (eg, company) [My Company Ltd]:PT. Ilusindo Karya Digital
Organizational Unit Name (eg, section) []:Information Technology
Common Name (eg, your name or your server's hostname) []:*.ilusidigital.com
Email Address []:ilusidigitalkita@gmail.com
Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []: biarkan kosong
An optional company name []: biarkan kosong
```

4. Salin file key agar nantinya passphrase bisa dihilangkan dengan perintah sebagai berikut :

```
cp ilusidigital.key ilusidigital.org
```

5. Hilangkan passphrase dengan perintah sebagai berikut :

```
openssl rsa -in ilusidigital.key.org -out ilusidigital.key
```

6. Hapus file key dengan passphrase karena sudah tidak diperlukan.

```
rm -f ilusidigital.key.org
```

7. Kirim file CSR dalam bentuk zip.

SSL - Create PEM

Urutan Value Pada File PEM untuk HAProxy / Lainnya.

1. CRT file -> ilusidigital.crt (Required)
2. Key file -> ilusidigital.key (Required)
3. Root CA/CRT file -> ilusidigital.ca (Required)
4. CSR file -> ilusidigital.csr (Optional)
5. Digicert CA file -> digicert.ca (Optional)

SSL - Let's Encrypt Nginx Ubuntu

Berikut adalah langkah-langkah untuk mengonfigurasi SSL Let's Encrypt di server Nginx :

1. Instal Certbot dan Plugin Nginx

Certbot adalah klien otomatis untuk memperoleh dan memperbarui sertifikat SSL dari Let's Encrypt. Pertama, Anda perlu menginstal Certbot dan plugin Nginx.

Pada distribusi berbasis Debian/Ubuntu, jalankan :

```
sudo apt update
sudo apt install certbot python3-certbot-nginx
```

2. Membuka Port 80 dan 443

Pastikan port 80 (HTTP) dan 443 (HTTPS) terbuka di firewall :

```
sudo ufw allow 'Nginx Full'
sudo ufw delete allow 'Nginx HTTP'
```

3. Mendapatkan Sertifikat SSL

Gunakan Certbot untuk mendapatkan sertifikat SSL untuk domain Anda. Gantikan ilusidgital.com dengan domain Anda, tambahakan -d jika ada domain tambahan lainnya :

```
sudo certbot --nginx -d ilusidigital.com -d www.ilusidigital.com
```

Certbot akan otomatis mengkonfigurasi Nginx untuk menggunakan sertifikat yang diperoleh.

4. Verifikasi Konfigurasi Nginx

Certbot akan memperbarui konfigurasi Nginx Anda untuk menggunakan sertifikat SSL yang diperoleh. Verifikasi bahwa konfigurasi telah diperbarui dengan benar dengan membuka file konfigurasi Nginx untuk domain Anda. Biasanya berada di /etc/nginx/conf.d/ilusidigital.conf.

Contoh blok server Nginx untuk HTTPS :

```
server {
    listen 443 ssl;
    listen [::]:443 ssl;
    server_name ilusidigital.com www.ilusidigital.com;

    ssl_certificate /etc/letsencrypt/live/ilusidigital.com/fullchain.pem;
    ssl_certificate_key /etc/letsencrypt/live/ilusidigital.com/privkey.pem;
    include /etc/letsencrypt/options-ssl-nginx.conf;
    ssl_dhparam /etc/letsencrypt/ssl-dhparams.pem;

    location / {
        proxy_pass http://localhost:3000;
        proxy_set_header Host $host;
        proxy_set_header X-Real-IP $remote_addr;
        proxy_set_header X-Forwarded-For $proxy_add_x_forwarded_for;
        proxy_set_header X-Forwarded-Proto $scheme;
    }
}
```

5. Mengatur Redirect HTTP ke HTTPS

Untuk mengarahkan semua lalu lintas HTTP ke HTTPS, tambahkan blok server berikut :

```
server {
    listen 80;
    listen [::]:80;
    server_name ilusidigital.com www.ilusidigital.com;

    location / {
        return 301 https://$host$request_uri;
    }
}
```

6. Restart Nginx

Setelah semua konfigurasi selesai, restart Nginx untuk menerapkan perubahan :

```
sudo systemctl restart nginx
```

7. Mengatur Pembaruan Otomatis Sertifikat

Let's Encrypt sertifikat hanya berlaku selama 90 hari. Untuk memastikan sertifikat Anda selalu diperbarui, tambahkan cron job untuk menjalankan pembaruan otomatis :

```
echo "0 3 * * * /usr/bin/certbot renew --quiet" | sudo tee -a /etc/crontab > /dev/null
```

8. Dengan langkah-langkah di atas, Anda akan memiliki server Nginx yang dikonfigurasi untuk menggunakan sertifikat SSL dari Let's Encrypt, memastikan bahwa komunikasi antara server dan klien dienkripsi dengan aman.

SSL - Let's Encrypt Nginx RockyLinux

Berikut adalah langkah-langkah untuk mengonfigurasi SSL Let's Encrypt di server Nginx :

1. Instal EPEL Repository dan Certbot

Anda perlu menginstal EPEL repository dan Certbot :

```
sudo dnf install epel-release
sudo dnf install certbot python3-certbot-nginx
```

2. Membuka Port 80 dan 443

Pastikan port 80 (HTTP) dan 443 (HTTPS) terbuka di firewall :

```
sudo firewall-cmd --permanent --add-service=http
sudo firewall-cmd --permanent --add-service=https
sudo firewall-cmd --reload
```

3. Mendapatkan Sertifikat SSL

Gunakan Certbot untuk mendapatkan sertifikat SSL untuk domain Anda. Gantikan ilusidgital.com dengan domain Anda, tambahakan -d jika ada domain tambahan lainnya :

```
sudo certbot --nginx -d ilusidigital.com -d www.ilusidigital.com
```

Certbot akan otomatis mengkonfigurasi Nginx untuk menggunakan sertifikat yang diperoleh.

4. Verifikasi Konfigurasi Nginx

Certbot akan memperbarui konfigurasi Nginx Anda untuk menggunakan sertifikat SSL yang diperoleh. Verifikasi bahwa konfigurasi telah diperbarui dengan benar dengan membuka file konfigurasi Nginx untuk domain Anda. Biasanya berada di /etc/nginx/conf.d/ilusidigital.conf.

Contoh blok server Nginx untuk HTTPS :

```
server {
    listen 443 ssl;
    listen [::]:443 ssl;
    server_name ilusidigital.com www.ilusidigital.com;

    ssl_certificate /etc/letsencrypt/live/ilusidigital.com/fullchain.pem;
    ssl_certificate_key /etc/letsencrypt/live/ilusidigital.com/privkey.pem;
    include /etc/letsencrypt/options-ssl-nginx.conf;
    ssl_dhparam /etc/letsencrypt/ssl-dhparams.pem;

    location / {
        proxy_pass http://localhost:3000;
        proxy_set_header Host $host;
        proxy_set_header X-Real-IP $remote_addr;
        proxy_set_header X-Forwarded-For $proxy_add_x_forwarded_for;
        proxy_set_header X-Forwarded-Proto $scheme;
    }
}
```

5. Mengatur Redirect HTTP ke HTTPS

Untuk mengarahkan semua lalu lintas HTTP ke HTTPS, tambahkan blok server berikut :

```
server {
    listen 80;
    listen [::]:80;
    server_name ilusidigital.com www.ilusidigital.com;

    location / {
        return 301 https://$host$request_uri;
    }
}
```

6. Restart Nginx

Setelah semua konfigurasi selesai, restart Nginx untuk menerapkan perubahan :

```
sudo systemctl restart nginx
```

7. Mengatur Pembaruan Otomatis Sertifikat

Let's Encrypt sertifikat hanya berlaku selama 90 hari. Untuk memastikan sertifikat Anda selalu diperbarui, tambahkan cron job untuk menjalankan pembaruan otomatis :

```
echo "0 3 * * * /usr/bin/certbot renew --quiet" | sudo tee -a /etc/crontab > /dev/null
```

8. Dengan langkah-langkah di atas, Anda akan memiliki server Nginx yang dikonfigurasi untuk menggunakan sertifikat SSL dari Let's Encrypt, memastikan bahwa komunikasi antara server dan klien dienkripsi dengan aman.

SSL - Let's Encrypt HAProxy Ubuntu

Berikut adalah tutorial lengkap untuk menginstal Let's Encrypt di Ubuntu dengan HAProxy:

1. Persiapan Awal

Pastikan Ubuntu server Anda sudah siap dan terhubung dengan internet. Anda juga perlu memastikan bahwa HAProxy sudah diinstal dan dikonfigurasi dengan benar.

2. Instal Certbot
Certbot adalah perangkat lunak yang digunakan untuk meminta dan mengelola sertifikat SSL dari Let's Encrypt.

Tambahkan Repositori Certbot :

```
sudo apt-get update
sudo apt-get install software-properties-common
sudo add-apt-repository universe
sudo add-apt-repository ppa:certbot/certbot
sudo apt-get update
```

Install Certbot :

```
sudo apt-get install certbot -y
```

3. Request Sertifikat SSL
Sekarang, mari kita minta sertifikat SSL dari Let's Encrypt untuk domain Anda.

Jalankan Certbot:

Untuk mendapatkan sertifikat SSL, Anda dapat menjalankan perintah berikut :

```
sudo certbot certonly --standalone -d ilusidigital.com -d www.ilusidigital.com
```

Gantilah `ilusdigital.com dan www.ilusidigital.com` dengan domain Anda akan gunakan. Certbot akan mencoba untuk menghubungi server Let's Encrypt, memverifikasi kepemilikan domain, dan

mengunduh sertifikat SSL.

Simpan Lokasi Sertifikat:

Certbot akan memberi tahu Anda di mana sertifikat dan kunci berada setelah berhasil. Biasanya, disimpan di `/etc/letsencrypt/live/ilusidigital.com/`.

4. Konfigurasi HAProxy

Sekarang kita akan mengkonfigurasi HAProxy untuk menggunakan sertifikat SSL yang baru saja kita dapatkan.

Buka File Konfigurasi HAProxy :

```
sudo nano /etc/haproxy/haproxy.cfg
```

5. Tambahkan Konfigurasi SSL di Frontend HAProxy:

Temukan bagian frontend di haproxy.cfg yang sesuai dengan konfigurasi situs web Anda dan tambahkan baris berikut untuk mengarahkan HAProxy menggunakan sertifikat SSL :

```
frontend http_front
    bind *:443 ssl crt /etc/letsencrypt/live/ilusidigital.com/fullchain.pem
    mode http
    option forwardfor
    option http-server-close
    ...
```

`bind *:443 ssl crt /etc/letsencrypt/live/ilusidigital.com/fullchain.pem`: Mengikat HAProxy ke port 443 dengan menggunakan sertifikat SSL dari Let's Encrypt.

Simpan dan Tutup File Konfigurasi:

Setelah mengedit `haproxy.cfg`, simpan dan tutup editor teks.

6. Restart HAProxy

Terakhir, restart HAProxy untuk menerapkan perubahan konfigurasi.

```
sudo systemctl restart haproxy
```

7. Otomatisasi Pembaruan Sertifikat

Agar sertifikat Let's Encrypt tetap terbarui secara otomatis, Anda dapat menambahkan tugas cron untuk menjalankan perintah pembaruan Certbot secara berkala.

Buka crontab untuk pengguna root :

```
sudo crontab -e
```

Tambahkan baris berikut untuk memperbarui sertifikat setiap minggu :

```
0 0 * * 0 certbot renew --quiet
```

Simpan dan tutup editor crontab.

8. Dengan langkah-langkah ini, Anda seharusnya berhasil menginstal dan mengkonfigurasi Let's Encrypt di HAProxy di server Ubuntu Anda. Pastikan untuk mengganti domainanda.com dengan domain yang sesuai dengan kebutuhan Anda.

SSL - Let's Encrypt HAProxy RockyLinux

Berikut adalah tutorial lengkap untuk menginstal Let's Encrypt di Ubuntu dengan HAProxy:

1. Persiapan Awal

Pastikan Rocky Linux server Anda sudah siap dan terhubung dengan internet. Anda juga perlu memastikan bahwa HAProxy sudah diinstal dan dikonfigurasi dengan benar.

2. Instal Certbot
Certbot adalah perangkat lunak yang digunakan untuk meminta dan mengelola sertifikat SSL dari Let's Encrypt.

Tambahkan Repositori Certbot :

```
sudo dnf install epel-release
```

Install Certbot :

```
sudo dnf install certbot -y
```

3. Request Sertifikat SSL
Sekarang, mari kita minta sertifikat SSL dari Let's Encrypt untuk domain Anda.

Jalankan Certbot:

Untuk mendapatkan sertifikat SSL, Anda dapat menjalankan perintah berikut :

```
sudo certbot certonly --standalone -d ilusidigital.com -d www.ilusidigital.com
```

Gantilah `ilusdigital.com dan www.ilusidigital.com` dengan domain Anda akan gunakan. Certbot akan mencoba untuk menghubungi server Let's Encrypt, memverifikasi kepemilikan domain, dan mengunduh sertifikat SSL.

Simpan Lokasi Sertifikat:

Certbot akan memberi tahu Anda di mana sertifikat dan kunci berada setelah berhasil. Biasanya, disimpan di `/etc/letsencrypt/live/ilusidigital.com/`.

4. Konfigurasi HAProxy

Sekarang kita akan mengkonfigurasi HAProxy untuk menggunakan sertifikat SSL yang baru saja kita dapatkan.

Buka File Konfigurasi HAProxy :

```
sudo nano /etc/haproxy/haproxy.cfg
```

5. Tambahkan Konfigurasi SSL di Frontend HAProxy:

Temukan bagian frontend di haproxy.cfg yang sesuai dengan konfigurasi situs web Anda dan tambahkan baris berikut untuk mengarahkan HAProxy menggunakan sertifikat SSL :

```
frontend http_front
    bind *:443 ssl crt /etc/letsencrypt/live/ilusidigital.com/fullchain.pem
    mode http
    option forwardfor
    option http-server-close
    ...
```

`bind *:443 ssl crt /etc/letsencrypt/live/ilusidigital.com/fullchain.pem`: Mengikat HAProxy ke port 443 dengan menggunakan sertifikat SSL dari Let's Encrypt.

Simpan dan Tutup File Konfigurasi:

Setelah mengedit `haproxy.cfg`, simpan dan tutup editor teks.

6. Restart HAProxy

Terakhir, restart HAProxy untuk menerapkan perubahan konfigurasi.

```
sudo systemctl restart haproxy
```

7. Otomatisasi Pembaruan Sertifikat

Agar sertifikat Let's Encrypt tetap terbarui secara otomatis, Anda dapat menambahkan tugas cron untuk menjalankan perintah pembaruan Certbot secara berkala.

Buka crontab untuk pengguna root :

```
sudo crontab -e
```

Tambahkan baris berikut untuk memperbarui sertifikat setiap minggu :

```
0 0 * * 0 certbot renew --quiet
```

Simpan dan tutup editor crontab.

8. Dengan langkah-langkah ini, Anda seharusnya berhasil menginstal dan mengkonfigurasi Let's Encrypt di HAProxy di server Ubuntu Anda. Pastikan untuk mengganti domainanda.com dengan domain yang sesuai dengan kebutuhan Anda.

SSL - Convert PBX

Berikut langkah-langkah lengkap (dengan perintah OpenSSL dan konfigurasi nginx) untuk mengambil isi dari file `.pfx` yang diproteksi password. Berikut langkah-langkah praktis dan langsung bisa dijalankan di server Linux (atau WSL/Git-Bash di Windows).

1. Periksa isi .pfx (opsional, hanya melihat)
akan diminta Import Password — masukkan password .pfx Anda

```
openssl pkcs12 -info -in mycert.pfx
```

2. Ekstrak private key (tanpa encrypt / tanpa passphrase) (Legacy Mode)
Note : **OpenSSL versi terbaru (3.x)** sudah *drop support* untuk algoritma lama RC2-40-CBC yang dipakai oleh Microsoft PFX. Jadi OpenSSL Anda tidak bisa membaca bagian CA chain (bagian PKCS7 Encrypted data).

```
openssl pkcs12 -in ilusi.pfx -nodes -legacy -out ilusi-all.pem
```

3. Pisahkan file hasil ekstrak

```
# Private key (BEGIN PRIVATE KEY sampai END PRIVATE KEY)
awk 'BEGIN {p=0} /BEGIN PRIVATE KEY/ {p=1} p; /END PRIVATE KEY/ {p=0}' ag-all.pem > key.pem


# Certificate (BEGIN CERTIFICATE sampai END CERTIFICATE)
awk 'BEGIN {p=0} /BEGIN CERTIFICATE/ {p=1; i++} p {print > "cert" i ".pem"} /END CERTIFICATE/ {p=0}' ag-all.pem
```

Hasilnya:

- `key.pem` → private key
- `cert1.pem` → biasanya **server certificate**
- `cert2.pem`, `cert3.pem` → biasanya **CA intermediate/root**

Gabungkan cert nya :

```
cat cert1.pem cert2.pem cert3.pem > fullchain.pem
```

4. Simpan ke lokasi standar

```
sudo mkdir -p /etc/ssl/private /etc/ssl/certs
sudo mv key.pem /etc/ssl/private/ilusi.key
sudo mv fullchain.pem /etc/ssl/certs/ilusi-fullchain.pem
```

```
sudo chmod 600 /etc/ssl/private/ilusi.key
sudo chmod 644 /etc/ssl/certs/ilusi-fullchain.pem
```