

**Administrasi Server Jaringan**  
***Hypertext Transfer Protocol Secure (HTTPS)***

**Khoirunnisa Fitria Aldira**

**19/XI KJ**

❖ Pengertian, port, protokol yang digunakan HTTPS

Pengertian : HTTPS adalah singkatan dari *Hypertext Transfer Protocol Secure* merupakan suatu protokol komunikasi dalam jaringan internet. HTTPS dapat diartikan sebagai bentuk protokol internet yang paling valid dan yang paling aman karena akan melindungi integritas serta kerahasiaan antara situs dan komputer pengguna.

Port : 443                      Protokol : TCP/IP

❖ Perbedaan HTTP dan HTTPS :

1. Keamanan data yang dikirimkan

HTTP tidak menjamin keamanan data yang ditransmisikan antara client dengan server. Sementara HTTPS menjamin keamanan data yang dikirimkan. Berbicara keamanan data, sedikitnya ada 3 aspek yang ditangani oleh HTTPS, yaitu:

- Autentikasi Server, dengan adanya autentikasi server, pengguna yakin sepenuhnya bahwa ia sedang berkomunikasi dengan server yang ia tuju.
- Kerahasiaan Data, data yang ditransmisikan tidak akan bisa dipahami oleh pihak lain, karena data yang ditransmisikan sudah dienkripsi.
- Integritas Data, data yang sedang ditransmisikan tidak dapat diubah oleh pihak lain, karena akan divalidasi oleh message authentication code (MAC).

2. Port yang digunakan

Untuk melakukan komunikasi, secara default HTTP menggunakan port 80 sedangkan HTTPS menggunakan port 443.

3. Kebutuhan SSL

Secara default, protokol yang digunakan untuk komunikasi client-server adalah HTTP. Sementara untuk dapat menggunakan protokol HTTPS, kita diharuskan memiliki sertifikat SSL. Secure Socket Layers (SSL) adalah teknologi keamanan yang memungkinkan untuk melakukan enkripsi terhadap data yang akan ditransmisikan antara client dan server. SSL memungkinkan kita untuk dapat mengirim informasi penting, seperti nomor kartu kredit dan login credential, dengan aman.

❖ Tutorial membuat HTTPS pada debian8 :

Disini telah diinstall DNS server dengan nama domain **alimrugi.com**

- Jika belum menginstall web server silahkan dengan perintah **apt-get install apache2 openssl ssl-cert**
- Untuk aplikasi web server sobat memerlukan DVD Binary 1

```
Enabling module authz_core.  
Enabling module authz_host.  
Enabling module authn_core.  
Enabling module auth_basic.  
Enabling module access_compat.  
Enabling module authn_file.  
Enabling module authz_user.  
Enabling module alias.  
Enabling module dir.  
Enabling module autoindex.
```

- Pastikan telah melakukan konfigurasi web server, disini telah dilakukan pengecekan melalui browser untuk domain **www.alimrugi.com**



- Selanjutnya ketikkan perintah

**openssl req -new -x509 -days 365 -nodes -out /etc/apache2/apache2.pem -keyout /etc/apache2/apache2.pem**

- Akan muncul isian seperti di bawah ini

```
root@debian:~# openssl req -new -x509 -days 365 -nodes -out /etc/apache2/apache2.pem -keyout /etc/apache2/apache2.pem  
Generating a 2048 bit RSA private key  
.....++++  
Enter new private key to '/etc/apache2/apache2.pem'  
-----  
You are about to be asked to enter information that will be incorporated  
into your certificate request.  
What you are about to enter is what is called a Distinguished Name or a DN.  
There are quite a few fields but you can leave some blank.  
For some fields there will be a default value,  
If you enter '.', the field will be left blank.  
-----  
Country Name (2 letter code) [AU]:ID  
State or Province Name (Full name) [Some-State]:Sulawesi Tengah  
Locality Name (eg, city) []:Buol  
Organization Name (eg, company) [Internet Widgits Pty Ltd]:PT.Alimrugi  
Organizational Unit Name (eg, section) []:Alimrugi  
Common Name (e.g. server FQDN or YOUR name) []:alimrugi.com  
Email Address []:admin@alimrugi.com
```

- Isi data di atas atau,
- Sobat bisa melewati tahapan isian dengan cara di enter

- Setelah itu aktifkan SSL dengan perintah **a2enmode ssl**

```
root@debian:~# a2enmode ssl
Considering dependency setenvif for ssl:
Module setenvif already enabled
Considering dependency ssl for ssl:
Module ssl already enabled
Considering dependency socache_shmcb for ssl:
Enabling module socache_shmcb.
Enabling module ssl.
See /usr/share/doc/apache2/README.Debian.gz on how to configure SSL and create a
self-signed certificates.
To activate the new configuration, you need to run:
service apache2 restart
root@debian:~#
```

- Lakukan restart untuk web server dengan perintah **service apache2 restart**
- Tambahkan script dibawah ini pada baris akhir file web sobat, disini file saya **web-alimrugi.conf** yang berada di **/etc/apache2/site-enabled**

LINUX<VirtualHost \*:443>

ServerName alimrugi.com

ServerAlias www.alimrugi.com

SSLEngine On

SSLCertificateFile /etc/apache2/apache2.pem

</VirtualHost>

- Simpan kemudian restart kembali web server apache2

## Tahapan pengujian konfigurasi HTTPS di Debian 8

Untuk melakukan pengujian, dapat anda buka url <https://www.alimrugi.com> melalui browser dari komputer client.





- Hasilnya yaitu anda berhasil merubah HTTP menjadi HTTPS tanpa Certificate Authority



Sumber:

- [https://www.codepolitan.com/mengetahui-perbedaan-http-dan-https#:~:text=Hypertext%20Transfer%20Protocol%20\(HTTP\)%20adalah,komunikasi](https://www.codepolitan.com/mengetahui-perbedaan-http-dan-https#:~:text=Hypertext%20Transfer%20Protocol%20(HTTP)%20adalah,komunikasi)

%20antara%20client%20dan%20server.&text=Sedangkan%20Hypertext%20Transfer%20Protocol%20Secure,dikembangkan%20oleh%20Netscape%20Communications%20Corp.

- <https://www.buatkuingat.com/2018/12/cara-mudah-konfigurasi-https-debian-8-server-pada-virtualbox.html?m=1>