

MODUL 13

OPENVPN (MULTI CLIENT)

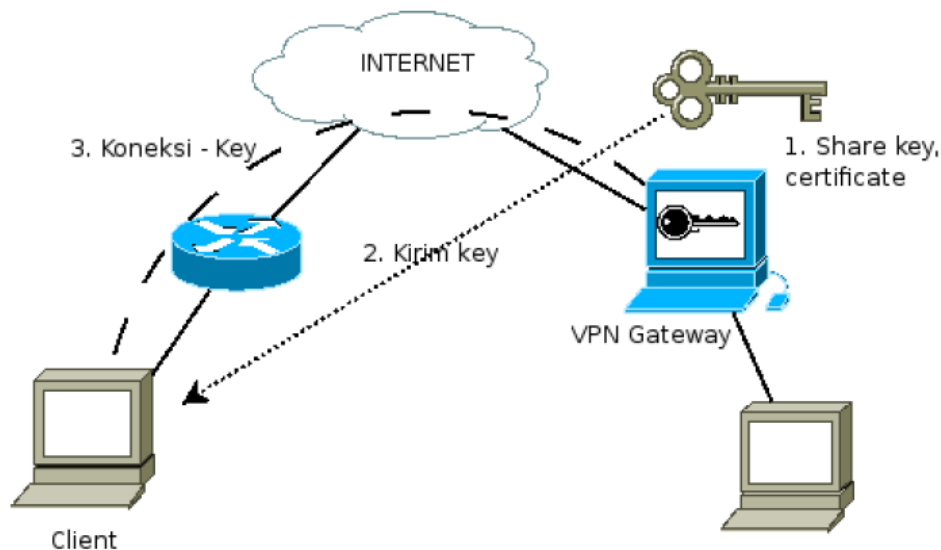
TUJUAN PEMBELAJARAN:

1. Mahasiswa mampu memahami cara kerja VPN dengan banyak client
2. Mahasiswa mampu menggunakan aplikasi VPN dengan banyak client
3. Mahasiswa mampu memahami troubleshoot jaringan VPN

DASAR TEORI

OpenVPN adalah aplikasi open source untuk Virtual Private Networking (VPN), dimana aplikasi tersebut dapat membuat koneksi point-to-point tunnel yang telah terenkripsi.

OpenVPN menggunakan private keys, certificate, atau username/password untuk melakukan autentikasi dalam membangun koneksi. Dimana untuk enkripsi menggunakan OpenSSL.



Gambar 1. Langkah-langkah VPN

Langkah-langkah membangun jaringan VPN adalah :

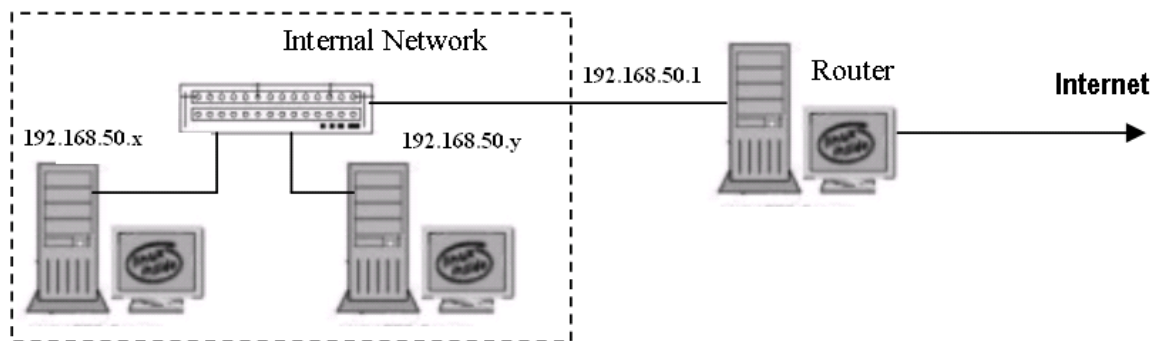
1. Pada VPN gateway membuat shared key dan certificate
2. Mengirimkan key tersebut kepada client yang akan melakukan koneksi
3. Membangun koneksi dengan menggunakan key yang telah didapat dari suatu VPN Gateway

TUGAS PENDAHULUAN

1. Jelaskan dengan singkat apa kegunaan dari VPN secara umum?
2. Jelaskan perbedaan VPN dan IPSec.

PERCOBAAN

1. Bangunlah jaringan seperti berikut :



Gambar 1 Jaringan Percobaan

NB:

Gunakan dhclient di masing-masing PC untuk mendapatkan IP dari router.

192.168.50.x & y : IP dari router

Pilih 192.168.50.x sebagai VPN Gateway

Pilih 192.168.50.y sebagai PC Client

A.KONFIGURASI BANYAK CLIENT DENGAN SERTIFIKAT YG SAMA

2. Pada VPN Gateway

- a. Install aplikasi openVPN

```
# apt-get install openvpn
```

- b. Mempersiapkan Certificate Authority (CA) dan Key

```
# cp /usr/share/doc/openvpn/examples/easy-rsa/ /root -Rf
```

```
# cd /root/easy-rsa/2.0
```

```
~/easy-rsa# source ./vars => konfigurasi dasar
```

```
~/easy-rsa# ./clean-all => menghapus konfigurasi lama di keys
```

```
~/easy-rsa# ./build-ca => buat sertifikat baru di keys
```

Pada perintah “build-ca”, akan muncul beberapa pertanyaan, isi dengan :

- Country Name : **ID**
- State or Province : **East Java**
- Locality Name : **Surabaya**
- Organization Name : **NetSecurity**
- Organization Unit : **VPN**
- Common Name : **VPN_Kelompok1** (isi dengan VPN Gateway)
- Email : **kel1@eepis-its.edu** (isi dengan email masing-masing)

- c. Membuat certificate dan key untuk server (VPN Gateway)

```
~/easy-rsa/2.0# ./build-key-server server
```

- Common Name : **Server_kelompok1**

Apabila ada pertanyaan password[], kosongkan. Sedangkan pada pertanyaan “Sign the certificate? [y/n]:” dan “1 out of 1 certificate requests certified, commit? [y/n]”, ketik y

- d. Membuat certificate dan key untuk banyak client
~easy-rsa/2.0# ./build-key client1

– Common Name : **Client1_kelompok1**

- e. Membuat Parameter dari Diffie Hellman
~easy-rsa/2.0# ./build-dh

- f. Pemindahan Keys dan Certificate
~easy-rsa/2.0# cp keys/ca.* /etc/openvpn
~easy-rsa/2.0# cp keys/server.* /etc/openvpn
~easy-rsa/2.0# cp keys/dh1024.pem /etc/openvpn

- g. Membuat konfigurasi untuk OpenVPN
#gunzip -c /usr/share/doc/openvpn/examples/sample-config-files/server.conf.gz >
/etc/openvpn/server.conf

#vim /etc/openvpn/server.conf

Rubah pada file konfigurasi /etc/openvpn/server.conf, pada bagian :

;local a.b.c.d

Dengan no IP dari VPN Gateway

local 192.168.50.10

Hilanglah komentar didepan baris duplicate-cn, ini digunakan jika key dan sertifikat sama diberikan untuk semua client.

;duplicate-cn

Menjadi

duplicate-cn

- h. Menjalankan openvpn

- Sebelum menjalankan openvpn, amatilah prosesnya dengan
tail -f /var/log/daemon.log
- Menjalankan OpenVPN dengan cara :
/etc/init.d/openvpn restart
- Sehingga akan muncul network device tun0:
ifconfig

3. Pada PC Client

- a. Install aplikasi openvpn
apt-get install openvpn

b. Salinlah file-file sertifikat dan kunci pada poin 2.d dari VPN Gateway ke semua PC Client yang akan melakukan koneksi ke VPN Gateway.

File yang perlu dicopy adalah :

ca.crt, ca.key, client1.crt, client1.csr dan client1.key

Gunakan aplikasi ftp/sftp untuk mencopy file-file diatas dari VPN Gateway, dan letakkan di **/etc/openvpn** di PC Client

```
# ftp <no_ip_VPN_Gateway>
>mget ca.*
>mget client1.*
>quit
```

```
# cp ca.* client1.* /etc/openvpn
```

c. Membuat konfigurasi untuk OpenVPN

Salin contoh file konfigurasi client.conf ke direktori /etc/openvpn, dengan cara

```
# cp /usr/share/doc/openvpn/examples/sample-config-files/client.conf /etc/openvpn/
```

Rubah file konfigurasinya dengan cara

```
# vim /etc/openvpn/client.conf
```

Pada bagian :

```
remote my-server-1 1194
```

Menjadi (192.168.50.10 adalah IP VPN Gateway)

```
remote 192.168.50.10 1194
```

Rubah bagian certificate dan key sesuai dengan file yang telah dibuat pada 3.b.

```
ca ca.crt
cert client1.crt
key client1.key
```

d. Menjalankan openvpn

Sebelum menjalankan openvpn, amatilah prosesnya dengan

```
# tail -f /var/log/daemon.log
```

Menjalankan OpenVPN dengan cara :

```
# /etc/init.d/openvpn restart
```

Sehingga akan muncul network device tun0:

```
# ifconfig
```

4. Tes koneksi

a. Lakukan ping dari semua PC Client ke VPN Gw : 192.168.50.10

b. Lakukan ping dari semua PC Client ke interface tun0 : 10.8.0.1

B.KONFIGURASI BANYAK CLIENT DENGAN SERTIFIKAT YG BERBEDA

5. Pada VPN Gateway

- a. Buat key dan certificate sebanyak client yang akan melakukan koneksi, dan buat nama yang berbeda-beda untuk masing-masing Common Name :

```
# cd /root/easy-rsa/2.0
```

```
~/easy-rsa# ./build-key client1 => untuk client 1
```

– Common Name : **Client1_kelompok1**

```
~/easy-rsa# ./build-key client2 => untuk client 2
```

– Common Name : **Client2_kelompok1**

```
~/easy-rsa# ./build-key client3 => untuk client 3
```

– Common Name : **Client3_kelompok1**

Filename	Needed By	Purpose	Secret
ca.crt	server + all clients	Root CA certificate	NO
ca.key	key signing machine only	Root CA key	YES
dh{n}.pem	server only	Diffie Hellman parameters	NO
server.crt	server only	Server Certificate	NO
server.key	server only	Server Key	YES
client1.crt	client1 only	Client1 Certificate	NO
client1.key	client1 only	Client1 Key	YES
client2.crt	client2 only	Client2 Certificate	NO
client2.key	client2 only	Client2 Key	YES
client3.crt	client3 only	Client3 Certificate	NO
client3.key	client3 only	Client3 Key	YES

- b. Menjalankan kembali OpenVPN :

```
# /etc/init.d/openvpn restart
```

6. Pada PC Client

- a. Salin file key dan certificate dari VPN Gateway ke PC Client sesuai dengan peruntukannya.

Misal

Untuk PC Client 1:

ca.crt, ca.key, client1.crt, client1.csr dan client1.key

Untuk PC Client 2:

ca.crt, ca.key, client2.crt, client2.csr dan client2.key

Untuk PC Client 3:

ca.crt, ca.key, client3.crt, client3.csr dan client3.key

b. Rubah file konfigurasinya dengan cara

```
# vim /etc/openvpn/client.conf
```

Rubah bagian certificate dan key sesuai di PC Client masing-masing, misal untuk PC Client 1

```
ca ca.crt
```

```
cert client1.crt
```

```
key client1.key
```

c. Menjalankan kembali OpenVPN :

```
# /etc/init.d/openvpn restart
```

7. Tes koneksi

a. Lakukan ping dari semua PC Client ke VPN Gw : 192.168.50.10

b. Lakukan ping dari semua PC Client ke interface tun0 : 10.8.0.1

C. KONEKSI ANTAR CLIENT

8. Lakukan ping antar PC Client.

9. Jika tidak bisa, setting di VPN Gateway sebagai berikut :

```
#vim /etc/openvpn/server.conf
```

Hilangkan komentar pada bagian :

```
client-to-client
```

10. Restart aplikasi openvpn

11. Lakukan kembali langkah 8.

LEMBAR ANALISA

Praktikum Network Security (OpenVPN – Multi Client)

Tanggal Praktikum :

Kelas :

Nama dan NRP :

A. Gambar topologi jaringan beserta dengan IP Addressnya, tunjukkan mana VPN Gateway dan PC Client

KONFIGURASI BANYAK CLIENT DENGAN SERTIFIKAT YG SAMA

B. Catat hasil pembuatan certificate authority (CA) pada poin 2.b

C. Catat hasil pembuatan certificate dan kunci untuk server (poin 2.c)

D. Catat hasil pembuatan certificate dan kunci untuk client (poin 2.d)

E. Catat proses yang terjadi saat openvpn diaktifkan di sisi server (poin 2.h)

E. Catat proses yang terjadi saat openvpn diaktifkan di sisi client (poin 3.d)

F. Catat hasil ping untuk tes koneksi pada poin 4 dengan sertifikat yang sama.

KONFIGURASI BANYAK CLIENT DENGAN SERTIFIKAT YG BERBEDA

G. Catat hasil ping untuk tes koneksi pada poin 7 dengan sertifikat yang berbeda.

INTERKONEKSI ANTAR CLIENT

H. Tes koneksi antar client pada jaringan VPN (poin 8 dan 11)