Praktikum Jaringan Komputer 2

Modul 5

OpenVPN

TUJUAN:

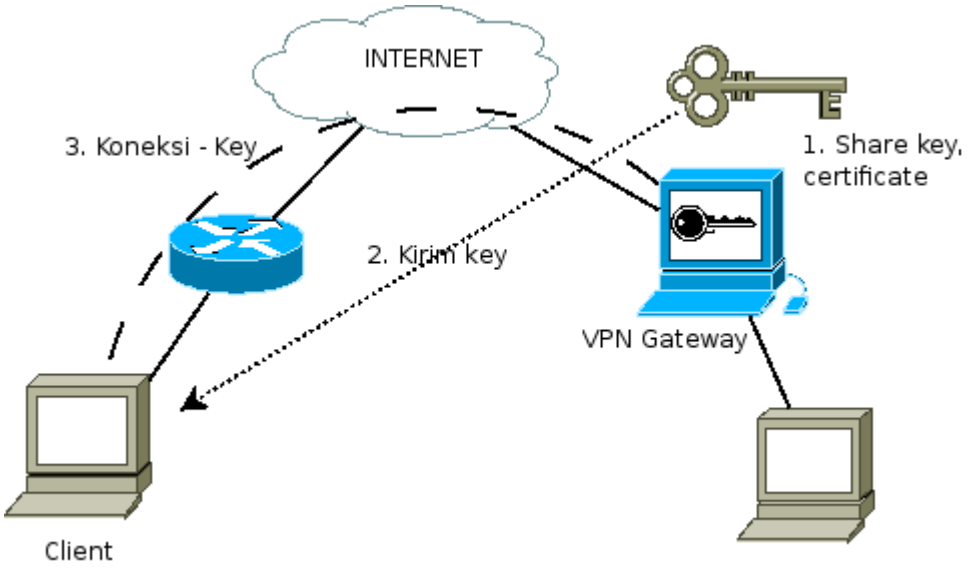
1. Mahasiswa mampu memahami cara kerja VPN
2. Mahasiswa mampu menggunakan aplikasi VPN
3. Mahasiswa mampu memahami troubleshot jaringan VPN

DASAR TEORI:

OpenVPN

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 authentikasi dalam membangun koneksi. Dimana untuk enkripsi menggunakan OpenSSL.



Gb 1. Langkang-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

Untuk menggunakan openVPN perlu dilakukan installasi, pada OS Debian dapat dilakukan dengan cara :

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

Mempersiapkan Certificate Authority (CA) certificate dan Key

Untuk mempersiapkan key pada openvpn dapat dilakukan dengan bantuan tools "easy-rsa", dimana tools tersebut terdapat di /usr/share/doc/openvpn/examples. Salin tools tersebut kedirektori /root, dengan cara

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

Kemudian gunakan tools tersebut dengan masuk ke direktori tersebut

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

Key dan certificate yang dibuat akan disimpan pada direktory "/root/easy-rsa/**keys**"

Untuk mengenerate CA dapat dilakukan dengan cara

```
~/easy-rsa# . ./vars
~/easy-rsa# ./clean-all
~/easy-rsa# ./build-ca
```

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

- Country Name : **ID**
- State or Province : **East Java**
- Locality Name : **Surabaya**
- Organization Name : **JARKOM2**
- Organization Unit : **VPN**
- Common Name : **router3.eepis-its.edu** (isi dengan VPN Gateway)
- Email : **admin@eepis-its.edu** (isi dengan email masing-masing)

Membuat certificate dan key untuk server (VPN Gateway)

Untuk membuat key dan certificate disisi server dapat dilakukan dengan cara :

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

Kemudian akan muncul beberapa pertanyaan yang mirip dengan perintah sebelumnya. Namun pada pertanyaan "Common Name" isikan dengan "nama server/router".

- Common Name : **router3.eepis-its.edu**

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**

Membuat certificate dan key untuk client

Untuk membuat key dan certificate yang akan digunakan oleh client, dapat dilakukan dengan cara :

```
~easy-rsa# ./build-key client
```

Kemudian akan muncul beberapa pertanyaan yang mirip dengan perintah sebelumnya. Namun pada pertanyaan "Common Name" isikan dengan "nama server/router".

- Common Name : **router3.eepis-its.edu**

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

Membuat Parameter dari Diffie Hellman

Parameter Diffie Hellman digunakan oleh 2 pengguna untuk melakukan pertukaran key rahasia melalui media yang tidak aman.

Untuk membuatnya dapat dilakukan dengan cara :

```
~easy-rsa# ./build-dh
```

Pemindahan Keys dan Certificate

Setelah membuat key dan certificate. Diperoleh key dan certificate yang disimpan di direktory “keys”

- ca.crt
- ca.key
- dhxxxx.pem, dimana xxxx adalah jumlah enkripsi yang digunakan
- server.crt
- server.csr
- server.key
- client.crt
- client.csr
- client.key

Kemudian pindahkan key dan certificate tersebut pada direktori /etc/openvpn, sedangkan **ca.crt, ca.key, client.crt, client.csr** dan **client.key** harus dipindah ke PC client yang akan membuat koneksi dengan VPN gateway.

Membuat konfigurasi untuk OpenVPN

Konfigurasi disisi VPN gateway menggunakan server.conf sedangkan disisi PC client adalah client.conf. Contoh file konfigurasi bisa diambil dari /usr/share/doc/openvpn/examples/sample-config-files/

Pada VPN gateway

Salin key dan certificate yang dibutuhkan (dh1024.pem, ca.* dan server.*). dengan cara :

```
~easy-rsa# cp keys/ca.* /etc/openvpn
~easy-rsa# cp keys/server.* /etc/openvpn
~easy-rsa# cp keys/dh1024.pem /etc/openvpn
```

Salin file konfigurasi ke direktori /etc/openvpn, dengan cara :

```
#gunzip -c /usr/share/doc/openvpn/examples/sample-config-files/server.conf.gz > /etc/openvpn/server.conf
```

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

```
;local a.b.c.d
```

Apabila IP dari VPN Gateway adalah 202.154.187.2 maka ganti a.b.c.d dengan 202.154.187.2. Sesuaikan dengan IP Router yang akan dijadikan VPN Gateway. Sehingga file tersebut dirubah menjadi:

```
local 202.154.187.2
```

Dengan menghilangkan tanda ; didepannya!!!
Menjalankan OpenVPN dengan cara :

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

Apabila sebelumnya, openvpn sudah berjalan. Lakukan :

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

Pada Client

Salin key dan certificate (ca.* dan client.*) dari server atau VPN Gateway yang diperlukan ke dalam direktori /etc/openvpn. Dapat dilakukan dengan mendownload atau mengambil dengan menggunakan protocol sftp.

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 :

```
remote 202.154.187.2 1194
```

Dimana 202.154.187.2 adalah IP server OpenVPN, ganti IP tersebut dengan IP VPN Gateway yang dituju.

Jalankan OpenVPN pada client dengan perintah :

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

Perangkat TUN

Pada server dan client setelah konfigurasi sempuma, akan muncul perangkat baru. Perangkat tersebut dapat dicek dengan perintah :

```
# ifconfig
```

```
tun0    Link encap:UNSPEC  HWaddr 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00
        inet addr:10.8.0.1  P-t-P:10.8.0.2  Mask:255.255.255.255
        UP POINTOPOINT RUNNING NOARP MULTICAST  MTU:1500  Metric:1
        RX packets:0 errors:0 dropped:0 overruns:0 frame:0
        TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
        collisions:0 txqueuelen:100
        RX bytes:0 (0.0 b)  TX bytes:0 (0.0 b)
```

PERALATAN:

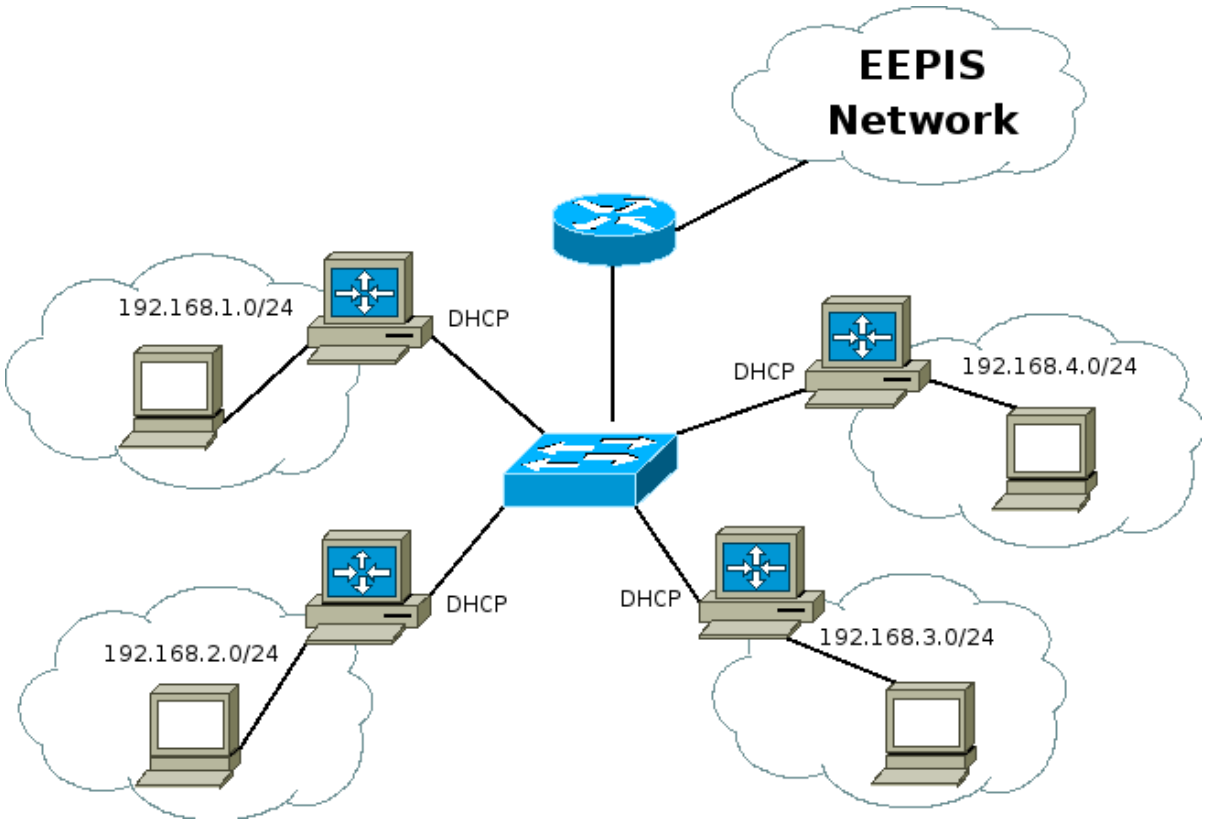
1. PC Router dengan 2 LAN Card atau lebih
2. PC Client
3. Switch
4. Aplikasi OpenVPN (linux / windows)

Catat semua langkah-langkah yang dilakukan praktikum pada laporan sementara !!!

LANGKAH-LANGKAH PRAKTIKUM:

Jaringan dengan NAT

1. Persiapkan jaringan sesuai dengan topologigambar



Gb 2: Topologi Praktikum OpenVPN

2. Set agar PC Router :
   - Interface ke arah switch menggunakan IP DHCP
   - Interface ke arah client menggunakan IP : 192.168.**1**.1 (khusus kelompok1)
   - Aktifkan IP_forward : # echo 1 > /proc/sys/net/ipv4/ip_forward
   - NAT, dengan cara : # iptables -t nat -I POSTROUTING -s 192.168.1.0/24 -j MASQUERADE

3. Set agar PC Client :
   - Menggunakan IP : 192.168.**1**.100 (khusus untuk kelompok1)
   - Default gateway kearah IP 192.168.**1**.1 (khusus kelompok1), dengan cara :

route add default gw 192.168.1.1

- Menggunakan DNS server 202.154.187.2, dengan cara :

echo “nameserver 202.154.187.2” > /etc/resolv.conf

4. Pastikan dari Client bisa ping ke arah server 202.154.187.2 !!!

OpenVPN

5. Lakukan installasi OpenVPN di PC Router dan Client
6. PC Router kelompok ganjil akan melakukan tunnel dengan client kelompok ganjil, begitu juga dengan kelompok genap !!!
7. Pada PC router akan bertindak sebagai VPN Gateway
8. Lakukan persiapan Certificate Authority (CA) di server
    1. Menyalin “easy-rsa”
    2. Membuat CA dengan menggunakan “build-ca”
    3. Membuat key dan certificate untuk server
    4. Membuat key dan certificate untuk client
    5. Membuat Diffie Hellman parameter
    6. Menyalin key dh1024.pem, ca.* dan server.* ke direktori /etc/openvpn
    7. Menyalin server.conf ke /etc/openvpn
    8. Rubah bagian “local”
    9. Jalankan openvpn
9. Lakukan persiapan di Client
    1. Ambil certificate dan key ca.* dan client.* dari server, letakkan di /etc/openvpn di PC Client
    2. Salin “client.conf” kedalam /etc/openvpn
    3. Rubah bagian “remote”
    4. Jalankan openvpn
10. Lakukan “ifconfig”, catat perangkat baru yang terbentuk dari OpenVPN
11. Lakukan mtr dari server ke client dan dari client ke server dengan menggunakan IP OpenVPN

REFERENSI

1. OpenVPN, http://www.openvpn.net
2. Wikipedia, http://www.wikipedia.org, “OpenVPN”