MODUL 8
VPN PADA CISCO ROUTER

TUJUAN PEMBELAJARAN:

1. Mengenalkan pada mahasiswa tentang VPN
2. Mengenalkan pada mahasiswa tentang konfigurasi VPN pada Cisco Router

DASAR TEORI

VPN (Virtual Private Network) dalam arti yang sederhana ialah koneksi secara logical yang menghubungkan dua node melalui public network. Koneksi logical tersebut bisa merupakan layer 2 ataupun layer 3 dalam basis OSI Layer. Begitu juga dengan teknologi VPN yang dapat diklasifikasikan atas Layer 2 VPN atau Layer 3 VPN. Secara konsep, baik Layer 2 VPN ataupun Layer 3 VPN ialah sama, yaitu menambahkan "delivery header" dalam paket data yang menuju ke site tujuan. Untuk Layer 2 VPN, delivery header-nya berada di Layer 2. Sedangkan untuk Layer 3, delivery header-nya berada di Layer 3. ATM dan Frame Relay adalah contoh dari Layer 2 VPN. GRE, L2TP, MPLS, dan IPSec adalah contoh dari Layer 3 VPN.

IPSec protocol diciptakan oleh kelompok kerja IPSec dibawah naungan IETF. Arsitektur dan komponen fundamental dari IPSec VPN seperti yang didefinisikan oleh RFC2401 adalah:

- Security protocols : Authentication Header (AH) dan encapsulation security payload (ESP)
- Key management : ISAKMP, IKE, SKEME
- Algorithms : enkripsi dan authentikasi

Enkripsi ialah proses transformasi dari plain text/data asli ke dalam data terenkripsi yang menyembunyikan data asli. Untuk melihat (dekripsi) data asli, penerima data yang terenkripsi harus mempunyai kunci/key yang cocok dengan yang telah didefinisikan oleh pengirim. Dekripsi ialah kebalikan dari enkripsi, yaitu proses transformasi dari data yang terenkripsi ke bentuk data asli.

Algoritma Kriptografi atau yang biasa disebut *cipher* adalah fungsi/perhitungan matematis yang digunakan untuk enkripsi dan dekripsi. Algoritma Kriptografi terbagi dua jenis:

- Symmetric
  Pada metode ini, pengirim maupun penerima menggunakan kunci rahasia yang sama untuk melakukan enkripsi dan dekripsi data. DES, 3DES, dan AES adalah beberapa algoritma yang popular
- Asymmetric
  Metode ini sedikit lebih rumit. Kunci untuk melakukan enkripsi dan dekripsi berbeda, kunci untuk melakukan enkripsi disebut public key sedangkan untuk dekripsi disebut private key.

Proses generate, distribusi, dan penyimpanan key disebut **key management**. Key management default dari IPSec ialah Internet Key Exchange Protocol (IKE). **Security Association** adalah blok basic dari IPSec yang juga merupakan input dari SA database (SADB) yang mengandung informasi tentang security yang telah disepakati untuk IKE atau IPSec. SA terdiri dari dua tipe:

- IKE atau ISAKMP SA
- IPSec SA

Untuk menuju IKE atau ISAKMP SA, IKE beroperasi dalam dua fase:

- **Fase 1**
  Fase ini menciptakan ISAKMP SA (atau sering juga disebut IKE SA) yang bertujuan menciptakan secure channel diantara IKE peers sehingga proses negoisasi fase 2 dapat berjalan lebih secure
- **Fase 2**
  Fase ini menyediakan proses negotiation dan establishment dari IPSec SA dengan menggunakan ESP atau AH untuk memproteksi lalu lintas data.

Konfigurasi IKE fase 1 pada Cisco IOS Router

```
Crypto isakmp policy 1
encr 3des
authentication pre-share
group 2
```

IKE fase 1 membutuhkan authentication method. Authentication method sendiri ada dua tipe, yaitu pre-shared key dan digital signatures.

Pre-shared key authentication
Pada metode ini, baik pengirim atau penerima harus mempunyai pre-shared key yang sama. Bila pre-shared key tidak sama, maka IKE Tunnel tidak akan terbentuk.

Konfigurasi pre-shared key pada Cisco IOS Router

```
Crypto isakmp key pre-shared_key address x.x.x.x
```

TUGAS PENDAHULUAN

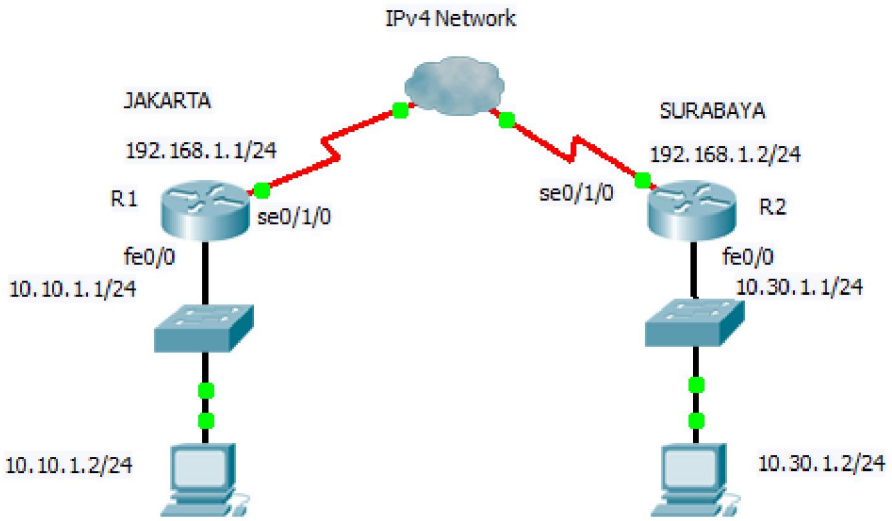
1. Jelaskan secara blok diagram antara symmetric dan asymmetric cryptography
2. Berikan contoh aplikasi nyata, jaringan yang menggunakan VPN

PERCOBAAN

A. Membangun Jaringan Tunneling

Untuk membangun simulasi ini ada beberapa langkah yang harus dilakukan untuk mendisain beberapa subnet jaringan berbasis IPv6 yang saling tehubung dalam satu jaringan melalui Ipv4.

1. Desain jaringan seperti gambar berikut:



Gambar 1. Desain Jaringan dengan VPN

Keterangan skenario gambar:

a. Pada gambar sekenario menunjukkan 2 subnet jaringan private yang berbeda, yaitu 10.10.1.0/24 dan 10.30.1.0/24 yang akan dihubungkan menggunakan VPN. Asumsikan 2 subnet jaringan tersebut terletak di Jakarta dan Surabaya, sedangkan IPv4 Network adalah jaringan milik ISP.

b. Masing-masing Router R1 dan R2 terhubung melalui kabel serial.

B. Konfigurasi pada Cisco Router untuk R1 (Jakarta)

2. Konfigurasi interface pada Router 1

a. Lakukan konfigurasi pada Router 1 dengan mengetikkan perintah berikut pada CLI:

```
R1> enable
R1#configure terminal
R1 (config)#interface fastethernet 0/0
R1 (config-if)#ip address 10.10.1.1 255.255.255.0
R1 (config-if)#no shutdown
R1(config-if)#exit

R1 (config)#interface serial 0/1/0
R1 (config-if)#ip address  192.168.1.1  255.255.255.0
R1 (config-if)#no shutdown
R1 (config-if)#exit
R1 (config)#
```

b. Untuk melihat hasil konfigurasi :

R1#show ip interface brief

Amati dan catat hasil perintah di atas.

3. **Konfigurasi Router 2**

a. Lakukan hal yang sama pada Router 2:

```
R2> enable
R2#configure terminal
R2 (config)#interface fastethernet 0/0
R2 (config-if)#ip address 10.30.1.1 255.255.255.0
R2 (config-if)#no shutdown
R2(config-if)#exit

R2 (config)#interface serial 0/1/0
R2 (config-if)#ip address  192.168.1.2  255.255.255.0
R2(config-if)#clock rate 64000                    => asumsi bahwa posisi DCE di R2
R2 (config-if)#no shutdown
R2 (config-if)#exit
R2 (config)#
```

b. Untuk melihat hasil konfigurasi ketikan sebagai berikut:

R2# show ip interface brief

Amati dan catat hasil perintah di atas.

4. Tahapan untuk melakukan tunneling dari R1 ke R2 dengan melewati jaringan IPv4. Untuk melakukannya lakukan langkah sebagai berikut pad CLI:

   a. **Pada Router 1:**

```
R1> enable
R1#configure terminal
Berikan access-list agar jaringan jkt-sby bisa saling interkoneksi
R1 (config)#ip access-list extended jkt-sby
R1 (config-ext-nacl)#permit ip 10.10.1.0  0.0.0.255  10.30.1.0  0.0.0.255
R1 (config-ext-nacl)#exit

Konfigurasi dengan VPN menggunakan isakmp, policy 1 adalah prioritasnya
R1 (config)#crypto isakmp policy 1
Enkripsi yang digunakan adalah triple DES, sebagai symmetric cryptography.
R1 (config-isakmp)#encr 3des
Authentication menggunakan pre-share key, dimana kedua kunci harus sama antara
jaringan Jakarta dan Surabaya
```

```
R1 (config-isakmp)#authentication pre-share
Untuk pertukaran kunci, digunakan Diffie Helman group 2
R1 (config-isakmp)#group 2
R1 (config-isakmp)#exit

Berikan nama kunci, dalam hal ini : vpnxyz  untuk koneksi ke 192.168.1.2 (Surabaya)
R1 (config)#crypto isakmp key vpnxyz address 192.168.1.2
Setting ipsec dengan nama transform-set : 6 dan protocol security yang digunakan
adalah esp-3des dan esp-sha-hmac
R1 (config)#crypto ipsec transform-set 6 esp-3des esp-sha-hmac
R1 (cfg-crypto-trans)#exit

Setting crypto map dengan nama : vpn-ngn dengan nomor urut 1
R1 (config)#crypto map vpn-ngn 1 ipsec-isakmp
Set koneksi ke jaringan 192.168.1.2 (Surabaya)
R1 (config-crypto-map)#set peer 192.168.1.2
Set transform-set : 6 (ini harus sesuai dengan settingan di atas)
R1 (config-crypto-map)#set transform-set 6
Set address : jkt-sby (ini harus sesuai dengan nama ACL)
R1 (config-crypto-map)#match address jkt-sby
R1 (config-crypto-map)#exit

Berikan crypto map di atas pada interface serial 0/1/0
R1 (config)#interface serial0/1/0
R1 (config-if)#crypto map vpn-ngn
R1 (config-if)#exit

Setting static route untuk koneksi dari Jakarta ke Surabaya
R1 (config)#ip route 10.30.1.0 255.255.255.0 192.168.1.2
R1 (config)#exit
```

b. Pada Router 2:

```
R2> enable
R2#configure terminal
Berikan access-list agar jaringan sby-jkt bisa saling interkoneksi
R2 (config)#ip access-list extended sby-jkt
R2 (config-ext-nacl)#permit ip 10.30.1.0  0.0.0.255  10.10.1.0  0.0.0.255
R2 (config-ext-nacl)#exit

Konfigurasi dengan VPN menggunakan isakmp
R2 (config)#crypto isakmp policy 1
R2 (config-isakmp)#encr 3des
R2 (config-isakmp)#authentication pre-share
R2 (config-isakmp)#group 2
R2 (config-isakmp)#exit
```

Berikan nama kunci, dalam hal ini : vpnxyz untuk koneksi ke 192.168.1.1 (Jakarta)

```
R2 (config)#crypto isakmp key vpnxyz address 192.168.1.1
R2 (config)#crypto ipsec transform-set 6 esp-3des esp-sha-hmac
R2 (cfg-crypto-trans)#exit
```

Setting crypto map dengan nama : vpn-ngn

```
R2 (config)#crypto map vpn-ngn 1 ipsec-isakmp
R2 (config-crypto-map)#set peer 192.168.1.1
R2 (config-crypto-map)#set transform-set 6
R2 (config-crypto-map)#match address sby-jkt
R2 (config-crypto-map)#exit
```

Berikan crypto map di atas pada interface serial 0/1/0

```
R2 (config)#interface serial0/1/0
R2 (config-if)#crypto map vpn-ngn
R2 (config-if)#exit
```

Setting static route untuk koneksi dari Jakarta ke Surabaya

```
R2 (config)#ip route 10.10.1.0 255.255.255.0 192.168.1.1
R2 (config)#exit
```

c. Untuk mengecek konfigurasi, ketikkan sebagai berikut:

Tabel routing

```
R1#show ip route
```

Policy pada isakmp

```
R1# show crypto isakmp policy
```

Koneksi antara Jakarta dan Surabaya

```
R1# show crypto isakmp sa
```

Pemetaan konfigurasi

```
R1# show crypto map
```

Protokol security yang digunakan

```
R1# show crypto ipsec transform-set
```

Amati dan catat hasilnya pada masing-masing router.

d. Untuk mengetahui jumlah paket yang dikirim, ketikkan perintah :

```
R1# show crypto ipsec sa
```

C. Konfigurasi pada PC Client

5. Lakukan setting secara manual pada PC Client
   a. Setting IP pada jaringan di Jakarta

```
# ifconfig eth0 10.10.1.2 netmask 255.255.255.0
```

   Tambahkan default gatewaynya :

```
# route  add –net default gw 10.10.1.1
```

   b. Lakukan setting juga pada client pada jaringan di Surabaya

```
# ifconfig eth0 10.30.1.2 netmask 255.255.255.0
```

   Tambahkan default gatewaynya :

```
# route  add –net default gw 10.30.1.1
```

   d. Lakukan ping dari jaringan di Jakarta ke jaringan di Surabaya, catat hasilnya

```
# ping  10.30.1.2
```

   e. Ulangi perintah 4.d, catat hasilnya dan amati perbedaannya.

LAPORAN RESMI

Berikan kesimpulan hasil praktikum yang anda lakukan.