

IPSec VPN pada Cisco Router

Herry Bayu Prasetyo

bayu.herry@gmail.com

herry.bayu@id.fujitsu.com

YM : herry_bayu

Lisensi Dokumen:

Copyright © 2003-2008 IlmuKomputer.Com

Seluruh dokumen di IlmuKomputer.Com dapat digunakan, dimodifikasi dan disebarkan secara bebas untuk tujuan bukan komersial (nonprofit), dengan syarat tidak menghapus atau merubah atribut penulis dan pernyataan copyright yang disertakan dalam setiap dokumen. Tidak diperbolehkan melakukan penulisan ulang, kecuali mendapatkan ijin terlebih dahulu dari IlmuKomputer.Com.

Apa itu VPN

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 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 autentikasi

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 populer
- **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. Artikel ini hanya membahas **pre-shared key**.

Pre-shared key authentication

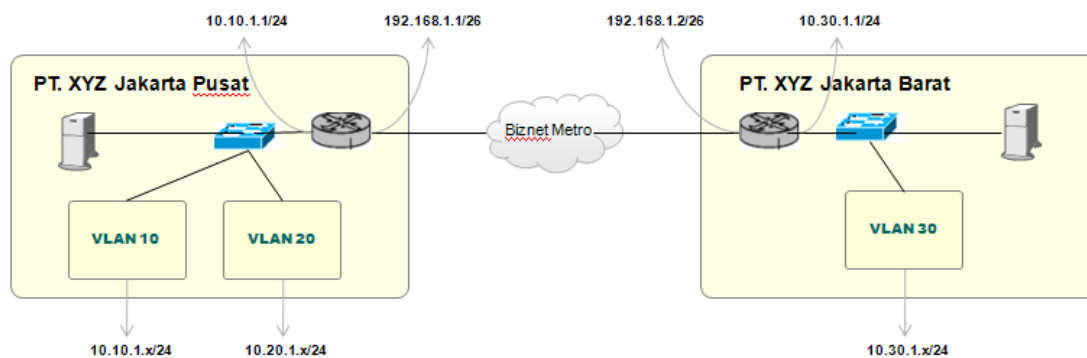
Pada metode ini, baik pengirim atau penerima harus mempunyai pre-shared key yang sama. Bila pre-shared key tidak sama, maka IKE Tunnel tidak akan terbentuk.

Konfigurasi pre-shared key pada Cisco IOS Router

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

Studi Kasus

PT. XYZ yang terletak di Jakarta Pusat ingin membuka cabang di Jakarta Barat. Untuk itu mereka ingin membangun koneksi yang aman dan terjamin kerahasiaannya antara kantor pusat dengan cabang tersebut melalui public network. Anda sebagai Network Engineer ditugaskan untuk membangun koneksi tersebut. Berikut ialah beberapa spesifikasi yang diberikan oleh PT. XYZ:



Gambar 1 PT. XYZ Network Topology

- ✓ Cisco Router 1841 (bundled VPN) (2 buah)
- ✓ Koneksi Biznet Metro WAN 1 Mbps (output kabelnya Ethernet Cat 5)
- ✓ Koneksi yang diizinkan antara Head Office dan branch hanya antara vlan 10 dan vlan 30
- ✓ Switch Jakarta Pusat : Cisco 3560
- ✓ Switch Jakarta Barat : Cisco 2960

Solusi Kasus

Konfigurasi Router A (Head Office - Jakpus)

```
ip access-list extended jakpus-to-jakbar
  permit ip 10.10.1.0 0.0.0.255 10.30.1.0 0.0.0.255

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

crypto isakmp key vpnxyz address 192.168.1.2
crypto ipsec transform-set 6 transvpnxyz esp-3des esp-sha-hmac
```

```
crypto map map-vpn-xyz 1 ipsec-isakmp
  set peer 192.168.1.2
  set transform set transvpnxyz
  match address jakpus-to-jakbar

Interface FastEthernet0/1
  Ip address 192.168.1.1 255.255.255.192
  crypto map map-vpn-xyz

Interface FastEthernet0/0
  Ip address 10.1.1.1 255.255.255.0

ip route 0.0.0.0 0.0.0.0 10.10.1.9 → IP Core Switch 3560
ip route 10.30.1.0 255.255.255.0 192.168.1.2
```

Konfigurasi Router B (Branch - Jakbar)

```
ip access-list extended jakbar-to-jakpus
  permit ip 10.30.1.0 0.0.0.255 10.10.1.0 0.0.0.255

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

crypto isakmp key vpnxyz address 192.168.1.1
crypto ipsec transform-set 6 transvpnxyz esp-3des esp-sha-hmac

crypto map map-vpn-xyz 1 ipsec-isakmp
  set peer 192.168.1.1
  set transform set transvpnxyz
  match address jakbar-to-jakpus

Interface FastEthernet0/1
  Ip address 192.168.1.2 255.255.255.192
  crypto map map-vpn-xyz

Interface FastEthernet0/0
  Ip address 10.30.1.1 255.255.255.0

ip route 0.0.0.0 0.0.0.0 1 192.168.1.1
```

Konfigurasi Switch Core 3560 (Head Office - Jakpus)

```
ip route 10.30.1.0 255.255.255.0 10.10.1.1
ip route 192.168.1.0 255.255.255.192 10.10.1.1
```

Testing Koneksi VPN

Berikut ini ialah command untuk memverifikasi koneksi VPN dari konfigurasi diatas

```
Router-A#show cry ipsec sa
interface: FastEthernet0/1
  Crypto map tag: map-vpn-xyz, local addr. 192.168.1.1
local ident (addr/mask/prot/port): (10.10.1.0/255.255.255.0/0/0)
remote ident (addr/mask/prot/port): (10.30.1.0/255.255.255.0/0/0)
current_peer: 192.168.1.2:500
  PERMIT, flags={origin_is_acl,}
  #pkts encaps: 10, #pkts encrypt: 10, #pkts digest 10
  #pkts decaps: 19, #pkts decrypt: 19, #pkts verify 19
  #pkts compressed: 0, #pkts decompressed: 0
  #pkts not compressed: 0, #pkts compr. failed: 0
  #pkts not decompressed: 0, #pkts decompress failed: 0
  #send errors 0, #recv errors 0
local crypto endpt.: 192.168.1.1, remote crypto endpt.: 192.168.1.2
  path mtu 1500, media mtu 1500
  current outbound spi: A8992968
  inbound esp sas:
    spi: 0xDFCB9E37(3754663479)
      transform: esp-3des esp-sha-hmac ,
      in use settings ={Tunnel, }
      slot: 0, conn id: 2000, flow_id: 1, crypto map: map-vpn-xyz
      sa timing: remaining key lifetime (k/sec): (4607997/3368)
      IV size: 8 bytes
      replay detection support: Y
  inbound ah sas:
  inbound pcp sas:
  outbound esp sas:
    spi: 0xA8992968(2828609896)
      transform: esp-3des esp-sha-hmac ,
      in use settings ={Tunnel, }
      slot: 0, conn id: 2001, flow_id: 2, crypto map: map-vpn-xyz
      sa timing: remaining key lifetime (k/sec): (4607998/3368)
      IV size: 8 bytes
      replay detection support: Y
  outbound ah sas:
  outbound pcp sas:
```

Referensi

1. Vijay Bollapragada, Mohamed Khalid, Scott Wainner, “*IPSec VPN Design*”, Cisco System, 2005
2. Pengalaman pribadi penulis

Biografi Penulis

Herry Bayu Prasetyo. Menyelesaikan S1 jurusan Teknik Informatika Universitas Gunadarma pada tahun 2007. Tahun 2006 bergabung bersama Binus Center sebagai Instruktur Network Administrator, mulai tahun 2007 sampai sekarang bekerja sebagai Network Engineer (Professional Service) di PT. Fujitsu Indonesia. Berpengalaman dalam menangani network, security, email server system, Active Directory dan Antivirus System di berbagai customer Fujitsu. Perusahaan tersebut antara lain Japan Embassy, PT. Bridgestone Tire Indonesia, PT Indomobil Suzuki Internasional, PT. JAS, PT. Aeon Credit Service Indonesia. Memegang sertifikasi CCNA dan FCNSA