BAB 2

LANDASAN TEORI

2.1 TEORI UMUM

2.1.1 VIRTUAL PRIVATE NETWORK (VPN)

Menurut (*http://computer.howstuffworks.com/VPN.htm* 23 Oktober 2012) teknologi *virtual private network* adalah sebuah *private network* yang bekerja menggunakan *public network* atau internet untuk menghubungkan *user* secara bersama-sama. VPN ini dibuat dengan tujuan dapat menghubungkan antar jaringan computer private secara aman dan dapat diandalkan melalui internet.

VPN memiliki kelebihan dan kekurangan, berikut adalah kelebihan dan kekurangan VPN:

Kelebihan

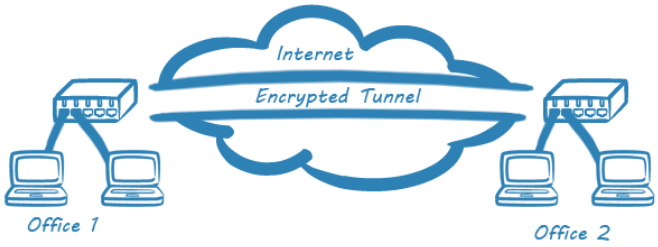
- Biaya relatif murah, karena tidak perlu membuat jalur pribadi hanya memanfaatkan jaringan internet publik
- Fleksibilitas, semakin berkembangnya internet dan banyaknya user yang menggunakannya membuat VPN juga berkembang
- Mengurangi kerumitan pengaturan dengan teknologi tunneling, tunneling merupakan kunci utama pada VPN. Koneksi pribadi dalam VPN dapat terjadi dimana saja selama terdapat tunnel yang menghubungkan pengirim dan penerima data.

Kekurangan

- VPN membutuhkan perhatian yang serius pada keamanan jaringan publik. Oleh karena itu diperlukan tindakan yang tepat untuk mencegah terjadinya hal-hal yang tidak diinginkan.
- Ketersediaan dan performasi jaringan khusus perusahaan sangat tergantung pada faktor-faktor yang berada di luar kendali pihak perusahaan, karena teknologi VPN ini memanfaatkan media internet.
- Ada kemungkinan perangkat pembangun teknologi jaringan VPN dari beberapa vendor yang berbeda tidak dapat digunakan secara bersama-sama.

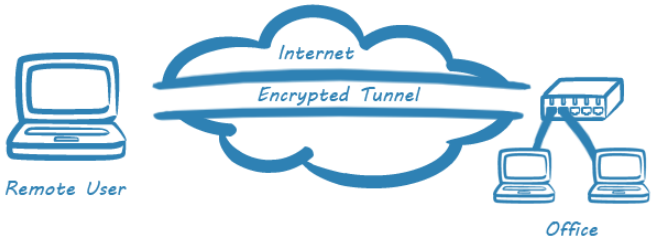
2.1.1.1 JENIS – JENIS VPN

1. Site-to-site VPN : merupakan suatu jaringan yang memungkinkan kantor-kantor yang berada di tempat berbeda dapat saling terhubung dengan aman melalui public network atau internet. *Site-to-site* VPN ini sangat cocok bagi perusahaan yang memiliki lusinan kantor cabang yang tersebar di seluruh dunia.



(Gambar 2.1 VPN *Site – to – Site*)

2. Remote-site VPN : mengizinkan user untuk melakukan hubungan yang aman dengan sebuah jaringan komputer. User tersebut dapat melakukan akses ke sumber-sumber data yang aman yang ada pada jaringan tersebut.VPN jenis ini memang cukup baik untuk user individual.



(Gambar 2.2 VPN *Remote - site*)

2.1.1.2 VPN TUNNELING PROTOCOL

Tunneling merupakan enkapsulasi dari paket atau paket didalam *frames*, seperti memasukan suatu amplop ke dalam amplop lain. *Tunneling* memegang peranan penting dalam penggunaan VPN, tetapi perlu diingat bahwa tunnels bukan merupakan VPN, dan VPN bukan merupakan tunnels.

Beberapa peran tersebut meliputi :

a) Menyembunyikan alamat *private*, *tunneling* menyembunyikan paket privat dan alamat tersebut di dalam paket alamat public, sehingga paket privat dapat melewati jaringan public.
b) Mengangkut muatan non-IP, *tunnel* sama dengan sirkuit virtual dimana paket non-IP dapat menjadi muatan untuk dapat diangkut melalui jaringan public seperti internet.
c) Fasilitas Data Shunting, memisahkan paket-paket data. Tunneling dapat meneruskan atau shunt seluruh paket langsung menuju ke lokasi spesifik.
d) Menyediakan keamanan, beberapa protokol tunneling menyediakan lapisan keamanan tambahan sebagai komponen tetap dari protokol.

Contoh – contoh protokol VPN tunneling:

1. IPSec

   IPSec didefinisikan secara resmi pertama kali di tahun 1995 dengan pengenalan '*Security Architecture for the Internet Protocol*' pada *Request for Comments* (RFC) 1825. IPSec menyediakan keutuhan dan kerahasiaan untuk paket IP. Sebagai sarana untuk menyediakan layanan tersebut, IPSec meliputi tida elemen dasar yang berguna sebagai protokol VPN, yaitu:

a) Otentikasi, memeriksa bahwa pengirim data merupakan pengirim itu sendiri bukan orang lain dan data yang dikirim sama dengan data yang diterima.
b) Enkripsi, mengacak data sehingga tidak dapat dimengerti oleh orang lain yang tidak mempunyai kunci yang tepat.
c) Penyesuaian kunci, menyesuaikan kunci antara pengirim dan penerima.

2. PPTP

Point – to – Point Tunneling Protocol (PPTP) digunakan untuk memfasilitasi pemindahan data secara aman dari klien ke server perusahaan melalui infrastruktur akses internet sebagai media transportasi umum.

3. L2TP

Layer 2 Tunneling Protocol (L2TP) merupakan hasil penggabungan dari spesifikasi PPTP dan L2F, dimana dapat mengenkapsulasi PPP frames dan mengantarkan data ke jaringan bersama (public).

4. GRE

Generic Routing Encapsulation (GRE) ditetapkan pada tahun 1994 dan merupakan salah satu pelopor protokol tunneling,

pada faktanya digunakan sebagai teknik enkapsulasi untuk protokol tunneling lainnya.

2.1.2 ROUTING

Routing adalah proeses memindahkan data dari satu *network* ke *network* lain dengan cara mem-*forward* paket data via *gateway*. Routing menentukan ke mana datagram akan dikirim agar mancapai tujuan yang diinginkan. Routing juga dapat diartikan sebagai suatu mekanisme yang digunakan untuk mengarahkan dan menetukan jalur mana yang akan dilewati paket paket dari satu *device* di satu jaringan ke *device* di jaringan lain berdasarkan informasi yang ada dalam tabel *routing*. Routing ada tiga macam cara yaitu *static routing*, *dynamic routing*, dan *default routing*. *Static routing* adalah mekanisme pengisian tabel *routing* secara manual oleh administrator pada masing-masing router. *Dynamic routing* adalah mekanisme pengisian dan pemeliharaan tabel *routing* secara terotomatisasi pada *router*. Default *routing* merupakan *routing* untuk paket yang alamat tujuannya tidak dikenal.

2.1.3 PENGALAMATAN IP

IP versi 4 memiliki pengalamatan terstruktur, terdiri dari 32 bit yang ditulis dalam nilai – nilai desimal yang dibagi dalam 4 segment dan setiap segmen terdiri dari 8 bit. IP address dapat ditulis dalam 8 bit (octet) angka binari atau angka decimal (0-255) yang dipisahkan oleh tanda titik. Contoh penulisan IP address dalam bentuk binari

11000000.00010000.00001010.00000001 atau dalam bentuk desimalnya 192.16.10.1. Alamat IP terdiri dari dua bagian yaitu network ID dan host ID. Dimana network ID menentukan alamat jaringan dan host ID menetukan alamat host atau komputer. Untul menentukan alamat kelas IP, dilakukan dengan memeriksa 4 bit pertama (bit yang paling kiri) dari alamat IP.

Kelas	4 Bit Pertama	Desimal
A	0xxx	1 – 126
B	10xx	128 – 191
C	110x	192 – 223
D	1110	224 – 239
E	1111	240 – 254

(Tabel 2.1 Kelas IP)

a) Kelas A

Bit pertama alamat IP kelas a adalah 0, network ID 8 bit dan panjang host ID 24 bit. Kelas A digunakan untuk jaringan yang berskala besar, terdapat 126 jaringan dan tiap jaringan dapat menampung hingga 16 juta host. Alamat IP kelas A dimulai dari 1.0.0.0 sampai dengan 126.255.255.255. alamat oktet awal 127 tidak boleh digunakan karena

digunakan unutk mekanisme Inter-process Communication di dalam perangkat jaringan yang bersangkutan.

b) Kelas B

Dua bit awal dari kelas B selalu diset 10 sehingga byte pertama kelas B bernilai antara 128-191. Network ID adalah 16 bit pertama dan host ID 16 bit sisanya. Kelas B digunakan untuk jaringan berskala menengah hingga besar, terdapat 16.384 jaringan dan tiap jaringan dapat menampung 65 ribu host. Alamat kelas B dimulai dari 128.0.0.0 sampai dengan 192.167.255.255.

c) Kelas C

Tiga bit awal dari kelas C selalu diset 110, sehingga byte pertama kelas C bernilai antara 192 – 223. Network ID adalah 24 bit dan host ID 8 bit sisanya. Kelas C biasa digunakan untuk jaringan kecil, terdapat 2.097.152 jaringan dan tiap jaringan dapat menampung 256 host. Alamat kelas C dimulai dari 192.168.0.0 sampai dengan 223.255.255.255

d) Kelas D

Empat bit awal dari kelas D selalu diset 1110, sehingga byte pertama kelas D bernilai antara 224 – 239. Kelas D digunakan untuk keperluan multicast, yaitu suatu metode

pengiriman yang digunakan bila suatu host ingin berkomunikasi dengan beberapa host sekaligus, dengan hanya mengirim satu datagram saja. Alamat dari kelass D adalah 224.0.0.0 sampai dengan 239.255.255.255. alokasi alamat tersebut ditujukan untuk keperluan sebuah grup, bukan untuk host seperti pada kelas A, B dan C.

e) Kelas E

Empat bit dari kelas E selalu diset 1111, sehingga byte pertama kelas E bernilai antara 240 – 254. Kelas E digunakan sebagai kelas eksperimental yang disiapkan untuk keperkuan di masa mendatang.

2.1.4 IP ADDRESS PRIVATE DAN PUBLIK

2.1.4.1 IP ADDRESS PRIVATE

Hampir seluruh alamat pada IPv4 merupakan alamat publik yang dapat digunakan pada jaringan internet, namun terdapat juga blok alamat yang digunakan untuk keperluan terbatas atau tidak terhubung dengan internet. Alamat tersebut disebut sebagai alamat private.

Range alamat private adalah:

- 10.0.0.0 – 10.255.255.255
- 172.16.0.0 – 172.31.255.255

- 192.168.0.0 – 192.168.255.255

Host – host yang tidak memerlukan akses ke internet dapat menggunakan alamat private sebanyak apapun. Namun, jaringan internal tetap harus didesain dengan pengalamatan yang baik dan terstruktur sehingga alamat yang digunakan tetap unik untuk network internal tersebut.

Host yang berada di jaringan yang berbeda dapat menggunakan alamat private yang sama. Paket yang menggunakan alamat tersebut sebagai *source* dan *destination* tidak akan muncul di jaringan internet. Router atau firewall yang terletak di ujung jaringan tersebut harus memblok atau menterjemahkan alamat – alamat tersebut.

2.1.4.2 IP ADDRESS PUBLIK

Umumnya alamat IPv4 merupakan alamat publik. Alamata tersebut didesain untuk digunakan pada host yang dapat diakses oleh host lain melalui internet.

2.1.5 ALGORITMA ROUTING

Algoritma routing (Tanenbaum, 2004, p264) adalah bagian dari perangkat lunak *network layer* yang bertanggung jawab untuk memutuskan jalur *output* pada paket yang telah ditransmisikan padanya.

Algoritma routing dibagi menjadi dua kelas utama, *adaptive* dan *non-adaptive*.

Adaptive algorithm merubah keputusan routing mereka sebagai cerminan perubahan yang terjadi dalam topologi, dan biasanya *traffic* juga. Adaptive algorithm berbeda dimana mereka mendapatkan informasi mereka (misal: dari router yang berdekatan), ketika mereka mengganti router (misal: ketika topologi berubah), dan metric yg digunakan untuk optimisasi (misal: jumlah hop).

Non-Adaptive algorithm keputusan routing tidak berdasarkan pada pengukuran atau perkiraan *traffic* dan *topology*.sebagai gantinya, pemilihan route di-*input* secara manual oleh *administrator* ke dalam *router* ketika jaringan sedang *boot*. Prosedur ini sering disebut *static routing*.

2.2 TEORI KHUSUS

2.2.1 VPN SITE – To – SITE

Merupakan suatu jaringan yang memungkinkan kantor-kantor yang berada di tempat berbeda dapat saling terhubung dengan aman melalui public network atau internet. *Site – to – site* VPN ini sangat cocok bagi perusahaan yang memiliki lusinan kantor cabang yang tersebar di seluruh dunia.

Ada dua jenis VPN *site – to – site*:

a. Intranet Based

Jika sebuah perusahaan memiliki satu atau lebih lokasi terpencil yang mereka ingin bergabung dalam private network, mereka dapat membuat VPN intranet untuk menghubungkan setiap LAN yang terpisah ke private WAN.

b. Extarnet Based

Ketika sebuah perusahaan memiliki hubungan dengan perusahaan lain (seperti pemasok, mitra atau pelanggan), dapat membangun VPN extranet yang menghubungkan LAN perusahaan – perusahaan tersebut. VPN extranet ini memungkinkan perusahaan untuk bekerja sama dalam menjaga jaringan bersama sambil mencegah akses ke intranet mereka yang terpisah.

2.2.2 SA (Security Assosiation)

Konsep SA (Davis, 2001, p186) adalah dasar dari IPSec. Kedua protokol yang IPSec gunakan AH dan ESP menggunakan SA, dan fungsi utama protokol IKE, protokol menjemen kunci yang menggunakan IPSec merupakan pembentukan dan pemeliharaan dari SA. SA adalah kesepakatan antara komunikasi pada protokol IPSec, mode operasi dari protokol (transport mode dan tunnel mode), algoritma enkripsi, kunci enkripsi dan masa pakai kunci yang akan digunakan untuk melindungi *traffic*. Jika keduanya, AH dan ESP yang diingkan untuk melindungi

traffic antara dua *peers*, maka dua set SA yang diperlukan, SA untuk AH dan satu lagi untuk ESP.

2.2.3 IPSec

IPSec (Forouzan, 2007, p841) adalah *framework* terbuka yang merinci aturan untuk komunikasi yang aman. Keamanan yang IPSec mampu sediakan melalui kombinasi dari protokol enkripsi dan mekanisme keamanan. IPSec memungkinkan sistem untuk memilih protokol keamanan yang diperlukan, memilih algoritma enkripsi yang diinginkan untuk digunakan dengan protokol yang dipilih dan menghasilkan kunci enkripsi apapun yang diperlukan untuk menyediaknan layanan yang diminta. IPSec menyediakan layanan enkripsi untuk keamanan transmisi data. IPSec bekerja pada network layer, melindungi, dan mengotentikasi paket IP yang sedang berkomunikasi.

Framework IPSec terdiri dari lima blok:

1. Protokol IPSec, meliputi AH dan ESP.
2. Jenis kerahasiaan yang diimplementasikan menggunakan algoritma enkripsi seperti DES, 3DES, AES. Pilihan penggunaan tergantung pada tingkat keamanan yang dibutuhkan.

3. Integritas yang dapat diimplementasikan baik menggunakan MD5 atau SHA.
4. Bagaimana *shared secret key* dibentuk. Kedua metode tersebut adalah pre-shared atau digitally signed (tandatangan digital) menggunakan RSA.
5. Merupakan kelompok algoritma Diffie-Hellman (DH). Ada empat algoritma pertukaran kunci yang terpisah yaitu DH kelompok 1 (DH1), DH kelompok 2 (DH2), DH kelompok 5 (DH5), DH kelompok 7 (DH7). Jenis kelompok yang dipilih tergantung pada kebutuhan tertentu.

IPSec dapat mengamankan jalur antara sepasang *gateway*, sepasang *host*, *gateway* dan *host*. Dengan menggunakan *framework* IPSec, IPSec menyediakan fungsi-fungsi keamanan penting sebagai berikut:

1. Confidentiality (kerahasiaan), untuk meyakinkan bahwa sulit untuk orang lain tetapi dapat dimengerti oleh penerima yang sah bahwa data telah dikirimkan. Contoh: Kita tidak ingin tahu seseorang dapat melihat password kerika login ke remote server.

2. Integrity (integritas), untuk menjamin bahwa data tidak berubah dalam perjalanan menuju tujuan.

3. Authenticity (otentikasi), untuk menandai bahwa data yang dikirimkan memang berasal dari pengiriman yang benar.

4. Secure key exchange, IPSec menggunakan algoritma DH untuk menyediakan metode pertukaran kunci public antara dua rekan untuk membentuk sebuah kunci rahasia bersama.

2.2.4 FUNGSI – FUNGSI KEAMANAN IPSec

Diatas sudah disebutkan fungsi – fungsi keamanan yang disediakan oleh IPSec. Berikut adalah penjelasan dari fungsi – fungsi keamanan IPSec.

1. Confidentiality (Kerahasiaan)

   Kerahasiaan didapat melalui enkripsi saat melewati VPN. Tingkat keamanan tergantung pada panjang kunci. Semakin pendek kuncinya, maka akan semakin mudah untuk dideskripsi. Algoritma enkripsi dan panjang kunci yang digunakan pada VPN yaitu seagai berikut.

   a. DES, Menggunakan kunci 56-bit memastikan enkripsi dengan performa yang tinggi. DES merupakan cryptosystem dengan kunci simetrik.

   b. 3DES, Sebuah variasi dari 56-bit DES. 3DES menggunakan tiga kunci enkripsi 56-bit setiap 64-bit blok, enkripsinya lebih kompleks dibandingkan dengan

DES. 3DES merupakan cryptosystem dengan kunci simetrik.

c. AES, Menyediakan keamanan yang lebih kompleks dibandingkan dengan DES dan lebih efisien dari pada 3DES. AES menawarkan tiga kunci yang berbeda: 128 bit, 192 bit, 256 bit. AES merupakan cryptosystem denagn kunci simetrik.

2. Integrity (Integritas)

Data yang diangkut melalui internat public berpotensi dapat dicegat dan dimodifikasi, oleh karena itu VPN merupakan suatu metode untuk membuktikan integritas data yang diperlukan untuk menjamin data belum diubah.

Hashed Message Authentication Codes (HMAC) adalah algoritma integritas data yang menjamin keutuhan pesan menggunakan nilai *hash*. Jika nilai *hash* yang dikirim sesuai dengan *hash* yang diterima, data merupakan data yang benar (tidak berubah). Akan tetapi, jika nilai *hash* yang dikirim tidak sesuai dengan nilai *hash* yang diterima, maka data tersebut tidak benar (telah berubah).

Secara umum, terdapat dua algoritma HMAC:

a. HMAC-Message Digest 5 (HMAC-MD5)

Menggunakan 128 bit shared secret key. Data denagn 128 bit shared secret key digabungkan dan dikirim dengan menggunakan algoritma HMAC-MD5, outputnya adalah 128 bit hash.

b. HMAC-Secure Hash Algoritm 1 (HMAC-SHA-1)

Menggunakan secret key 160 bit. Data dengan 160 bit shared secret key digabungkan dan dikirim dengan menggunakan algoritma HMAC-SHA-1, ouputnya adalah 160 bit hash.

3. Authentication (otentikasi)

Apabila melakukan pertukaran data jarak jauh melalui e-mail atau fax perlu mengetahui (otentikasi) pihak penerima. Hal ini berlaku juga untuk VPN, pihak penerima harus dipastikan harus dipastikan terlebih dahulu sebelum jalur komunikasi dianggap aman. Para era elektronik, data ditandai menggunakan *private encryption key* dari pengirim yang disebut digital signature. Digital signature tersebut dibuktikan melalui deskripsi menggunakan public key dari pengirim.

Terdapat dua metode untuk menkonfigurasi otentikasi *Peer – to – Peer*.

a. Pre-shared Key (PSK)

Sebuah *pre-shared secret key* dimasukkan kedalam setiap *peer* secara manual dan digunakan untuk membuktikan (otentikasi) *peer* tersebut. Setiap *peer* harus memastikan setiap penarima sebelum *tunnel* dianggap aman.

b. RSA signature

Pertukaran sertifikat digital mengotentikasikan *peer*. Perangkat lokal membawa sebuah *hash* dan mengenkripsinya menggunakan private key. Hash yang terenkripsi dilampirkan ke dalam pesan dan diteruskan ke penerima dan bertindak seperti sebuah signature. Pada penerima, *hash* yang terenkripsi dideskripsikan menggunakan public key. Jika hasil deskripsi *hash* sama dengan *hash* awal, maka signature tersebut asli. Setiap *peer* memastikan setiap penerima sebelum *tunnel* dianggap aman.

4. Secure Key Exchange

Algoritma enkripsi seperti DES, 3DES, dan AES serta algoritma hashing MD5 dan SHA-1 memerlukan sebuah simetrik yaitu *shared secret key* untuk melakukan enkripsi dan deskripsi.

E-mail, courier, atau overnight express dapat digunakan untuk mengirimkan *shared secret key* kepada administrator, tetapi

metode pertukaran kunci paling mudah adalah dengan metode pertukaran public key antara perangkat enkripsi dan dekripsi.

Kunci Diffie-Hellman (DH) adalah metode pertukaran public key yang menyediakan sebuah cara bagi dua *peer* untuk membuat *shared secret key* yang hanya diketahui oleh kedua *peer* tersebut, meskipun kedua *peer* tersebut melakukan komunikasi di saluran yang tidak aman.

2.2.5 IPSec SECURITY PROTOCOL

IPSec merupakan (Forouzan, 2007, p842) framework standar terbuka. IPSec menguraikan pesan untuk mengamankan komuniksi, tetapi bergantung pada algoritma yang ada. Dua protokol framework utama IPSec adalah AH dan ESP. Pemilihan dari salah satu protokol tersebut berpengaruh pada blok Framework lain yangtersedia:

1. Authentication header (AH)

   Untuk memastikan penggunaan fitur verifikasi identitas pengirim pesan.

2. Encapsulating Security Protocol (ESP)

   Memastikan kerahasiaan (confidentiality) data itu sendiri.

AH dan ESP dapat diterapkan untuk paket IP dalam dua mode yang berbeda, transport mode dan tunnel mode :

1. Transport Mode

Keamanan disediakan hanya untuk transport layer ke atas dari model OSI. Transport mode melindungi muatan data dari paket tetapi meninggalkan alamat IP asli dalam plaintext. Alamat IP asli digunakan untuk mengarahkan paket melalui internet.

ESP transport mode digunakan antar host. Transport mode bekerja baik dengan GRE, karena GRE menyembunyikan alamat penerima dengan menambahkan IP dirinya sendiri.

2. Tunnel Mode

Tunnel mode menyediakan keamanan untuk paket IP lengkap yang asli. Paket IP yang asli dienkripsi dan kemudian dirumuskan dalam paket IP yang lain. Alamat IP pada paket IP luar digunakan untuk mengarahkan paket melalui internet. ESP *tunnel mode* digunakan antara *security host* dan *gateway* atau antara dua *security gateway*.

2.2.6 INTERNET KEY EXCHANGE

Solusi IPSec VPN memerlukan parameter pertukaran kunci, menentukan *shared key*, mengotentikasikan *peer*, dan negosiasi parameter kunci enkripsi. Negosiasi antara kedua parameter kunci enkripsi dikenal juga dengan *Security Association* (SA).

2.2.7 PERANGKAT SSG (SECURE SERVICE GATEWAY)

SSG khusus dibuat untuk memberikan *high performance paltforms* konektivitas dan keamanan WAN, ditambah untuk melindungi *high-speed* LAN terhadap jaringan internal dan serangan aplikasi bertingkat sekaligus menghentikan konten yang berbasis serangan. Selain itu SSG juga menyediakan seperangkat *Unified Threat Management* (UTM) fitur keamanan termasuk Firewall, IPSec VPN, IPS, Antivirus (antispyware, antiphishing), Anti-spam, dan Web filtering. Manajemen komfigurasi melalui UI Web, CLI, atau NSM pusat sistem manajemen.

Tipe perangkat SSG yang digunakan adalah SSG5 dan SSG20:

1. **SSG5**

   SSG5 dibangun bertujuan untuk keamanan platform VPN yang tetap, dengan efektif dapat memberikan 160Mbps dari traffic firewall dan 40Mbps dari throughput VPN IPSec untuk *small branch*, *teleworker* dan *enterprise deployment* (juniper.net/us/en/products-services/security/ssg-series).

(Gambar 2.3 SSG5)

2. SSG20

SSG20 dibangun bertujuan untuk keamanan platform VPN modular, dengan efektif dapat memberikan 160Mbps dari traffic firewall dan 40Mbps dari throughput VPN IPSec untuk *small branch*, *teleworker* dan *enterprise deployment* (juniper.net/us/en/products-services/security/ssg-series).

(Gambar 2.4 SSG20)

2.2.8 MPLS (Multiprotocol Label Switching)

Multiprotocol Label Switching (MPLS) adalah sebuah metode dengan performa tinggi untuk meneruskan paket melewati suatu jaringan. MPLS mengizinkan router yang berada di edge network untuk menyisipkan label yang simple kedalam sebuah paket (Cisco Sistems Learning 2011).

Prinsip kerja MPLS menggabungkan kecepatan *switching* pada *layer 2* dengan kemampuan *routing* dan skalabilitas pada *layer 3*. Cara kerjanya adalah dengan menyelipkan *label* di antara *header layer 2* dan *layer 3* pada paket yang diteruskan. Label dihasilkan oleh *Label-Switching Router* dimana bertindak sebagai penghubung jaringan MPLS

dengan jaringan luar. *Label* berisi informasi tujuan *node* selanjutnya kemana paket harus dikirim. Kemudian paket diteruskan ke *node* berikutnya, di *node* ini label paket akan dilepas dan diberi label yang baru yang berisi tujuan berikutnya.

2.2.9 STATIC ROUTE

Static route digunakan dalam sebuah jaringan yang hanya terdiri dari beberapa *router* saja atau dipakai untuk jaringan kecil dan jaringan yang terhubung ke internet hanya melalui satu *Internet Service Provider* (ISP). Digunakan *static route* kerena hanya *Internet Service Provider* tersebut yang menjadi jalan keluar untuk akses ke internet.

Dalam *static route*, pengisian dan pemeliharaan *routing table* yang berisi informasi dilakukan secara manual oleh administrator. Administrator mengisi setiap *route* tujuan kedalam tabel. Ketika menggunakan tabel tipe ini, jika terjadi perubahan pada *internet* tidak terjadi update secara otomatis pada *routing table*. *Static routing table* bisa digunakan pada internet skala kecil yang tidak membutuhkan perubahan sangat sering. Sangat tidak disarankan untuk menggunakan *static table routing* pada internet yang besar.

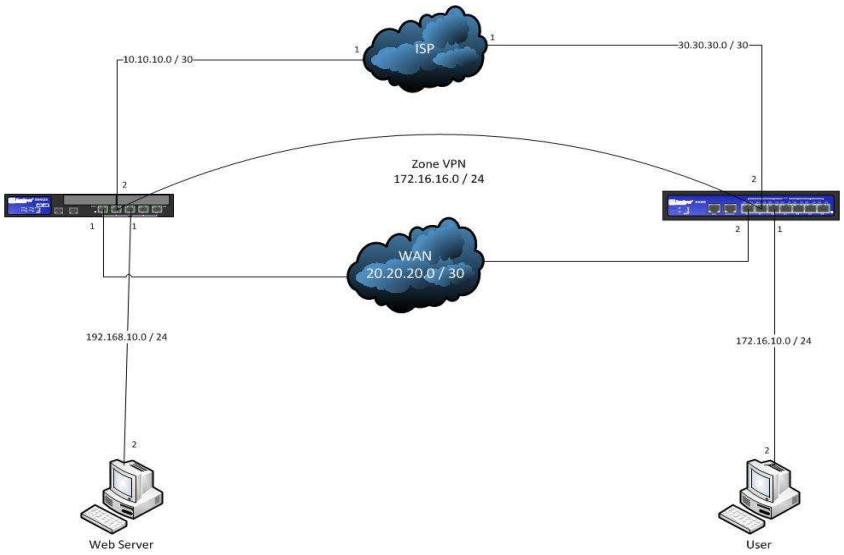
Kelebihan dalam *static route* yaitu tidak memerlukan *bandwith* jaringan yang besar akan tetapi bisa mencari alternative jalan baru untuk meneruskan paket data yang dikirim.

2.2.10 FAILOVER

Menurut (http://searchstorage.techtarget.com 23 Oktober 2012) *Failover* adalah mode operasional cadangan di mana fungsi dari komponen sistem (seperti prosesor, server, jaringan, atau database, misalnya) yang diasumsikan dengan komponen sekunder ketika komponen utama menjadi tidak tersedia akibat salah satu kegagalan atau *downtime* yang telah dijadwalkan. Digunakan untuk membuat sistem yang lebih (fault-tolerant) toleransi terhadapat kegagalan.

2.2.10.1 MENGAPA FAILOVER?

Failover dalam istilah *computer internetworking* adalah kemampuan sebuah sistem untuk dapat berpindah secara manual maupun otomatis jika salah satu sistem mengalami kegagalan sehingga menjadi *backup* untuk sistem yang mengalami kegagalan.



(Gambar 2.5 Konsep *Failover*)

Untuk mempermudah dan memperjelas maksud *failover* dapat melihat contoh gambar 2.3. pada gambar tersebut dapat dilihat sebuah topologi jaringan yang menggunakan lebih dari satu ISP. Jaringan web server dengan ip 192.168.10.2/24 menggunakan WAN sebagai jalur utama untuk komunikasi dengan User dengan ip 172.16.10.2/24. Jika WAN mengalami disconnect (putus) maka ISP backup akan menggantikan WAN. Jika WAN sudah kembali normal maka jalur koneksi yang digunakan kembali menjadi WAN.

Dengan begitu dapat disimpulkan bahwa tujuan dari failover kali ini adalah digunakan untuk menggantikan atau sistem backup koneksi isp yang terputus dengan koneksi isp yang lainnya.

2.2.10.2 SISTEMATIKA PENGUJIAN FAILOVER

Untuk dapat mengetahui teknik *failover* telah bekerja maka harus dilakukan pengujian dengan cara memutuskan salah satu jarinagn ISP yaitu dengan mencabut kabel *ethernet* atau dengan cara men*disable* salah satu jaringan ISP dengan cara mengkonfigurasi pada *router* juniper. Apabila setelah salah satu jalur ISP diputus dan ISP yang lain dapat menggantikannya maka teknik *failover* telah berhasil diterapkan pada sistem tersebut.

2.2.10.3 Network Address Translation (NAT)

Network Address Translation (NAT) adalah suatu metode untuk menghubungkan lebih dari satu komputer ke jaringan internet dengan menggunakan satu alamat IP. Banyaknya penggunaan metode ini disebabkan karena ketersediaan alamat IP yang terbatas, kebutuhan akan keamanan (security) dan kemudahan serta fleksibilitas dalam administrasi jaringan. Saat ini, protokol IP yang banyak digunakan adalah IP versi 4 (IPv4). Dengan panjang alamat 4 byte berarti terdapat 2^{32} = 4.294.967.296 alamat IP yang tersedia. Jumlah ini secara teoritis adalah jumlah komputer yang dapat langsung koneksi ke internet. Karena keterbatasan inilah sebagian besar ISP (*Internet Service Provider*) hanya akan mengalokasikan satu alamat untuk satu pengguna dan alamat ini bersifat dinamik, dalam arti alamat IP yang diberikan akan berbeda setiap kali user melakukan koneksi ke internet. dengan NAT *gateway* yang dijalankan di salah satu komputer, satu alamat IP tersebut dapat dibagi ke beberapa komputer yang lain dan mereka bisa melakukan koneksi ke internet secara bersamaan.

Proses dari *Network Address Translation* (NAT) atau dikenal dengan nama *network mesquerading* atau *IP-mesquerading* mengakibatkan penulisan alamat ulang sumber dan atau tujuan dari paket IP ketika melewati *router* atau *firewall*.

Network Address Translation terdiri dari berbagai jenis, yaitu:

1. Static NAT

   Network Address Translation (NAT) menerjemahkan sejumlah IP *address* tidak terdaftar menjadi sejumlah IP *address* yang terdaftar sehingga setiap *client* dipetakkan kepada IP *address* terdaftar dengan jumlah yang sama.

   Jenis NAT ini merupakan pemborosan IP *address* terdaftar, karena setiap IP *address* yang tidak terdaftar (un-registered IP) dipetakkan kepada satu IP *address* terdaftar. Statik NAT ini juga tidak seaman jenis NAT lainnya, karena setiap komputer secara permanen diasosiasikan kepada *address* terdaftar tertentu, sehingga memberikan kesempatan kepada para penyusup dari internet untuk menuju langsung kepada komputer tertentu pada *private network* anda menggunakan *address* terdaftar tersebut. Contoh:

   Pada statik NAT, komputer dengan IP address 192.168.32.10 selalu di translate ke IP address 213.18.123.110.

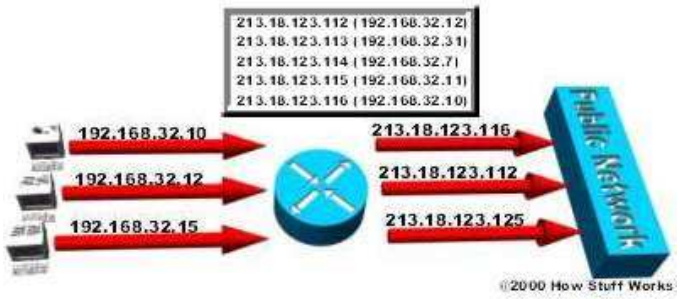
(Gambar 2.6 NAT *Static*)

2. Dynamic NAT

Dynamic Network Address Translation dimaksudkan untuk suatu keadaan dimana anda mempunyai IP *address* terdaftar yang lebih sedikit dari jumlah IP *address un-registered*. *Dynamic* NAT menerjemahkan setiap komputer dengan IP tak terdaftar kepada salah satu IP address terdaftar untuk konek ke internet. Hal ini agak menyulitkan para penyusup untuk menembus komputer didalam jaringan anda karena IP *address* terdaftar yang diasosiasikan ke koputer selalu berubah secara dinamis, tidak seperti pada NAT statik. Kekurangan utama dari *dynamis* NAT ini adalah bahwa jika jumlah IP address terdaftar sudah terpakai semuanya, maka untuk komputer yang berusaha konek ke internet tidak lagi bisa karena IP *address* terdaftar sudah terpakai semuanya. Contoh:

Pada *dynamis* NAT, komputer dengan IP *address* 192.168.32.10 akan di *translate* ke IP *address* yang

tersedia pertama kali dari rentang IP *address* 213.18.123.100 – 213.18.123.150.



(Gambar 2.7 NAT *Dynamic*)