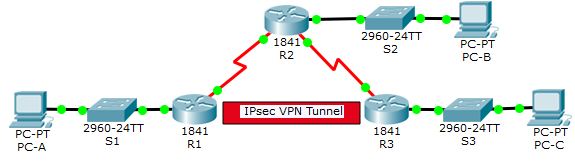
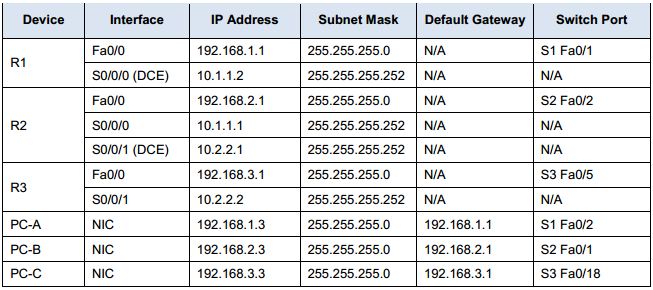
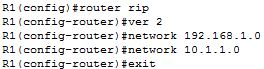
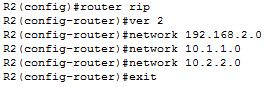
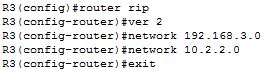
**LAPORAN PRAKTIKUM KEAMANAN JARINGAN 2**

**UNIT 7**



Pada praktikum kali ini, dibuat topologi seperti gambar di atas, dengan menggunakan tiga router, tiga switch, dan tiga PC. Semua device tersebut diberikan IP address sesuai dengan IP table di atas. Kemudian, konfigurasikan ketiga router dengan protokol RIP versi 2.



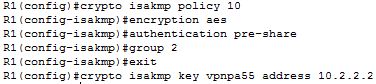
Selanjutnya, tes koneksi dengan melakukan ping dari PC-A ke PC-C.

1.JPG

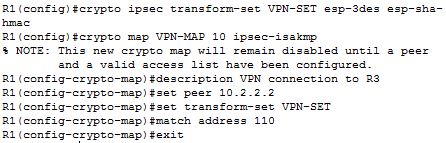
Lalu, buat access list 110 pada R1 untuk mengeidentifikasi traffic LAN pada R1 ke LAN pada R3. Semu traffic yang bersumber dari LAN tidak akan terenkripsi. Access list 110 akan mengizinkan IP pada network 192.168 1.0 dengan IP wildcard 0.0.0.255 untuk mengakses IP pada network 192.168.3.0 dengan IP wildcard 0.0.0.255.

2.JPG

Kemudian, konfigurasi isakmp phase 1 pada R1. Dibuat crypto isakmp policy dengan name 10, lalu dikonfigurasi dengan enkripsi aes dan autentikasi pre-share. Setelah itu, dibuat grup untuk dapat melakukan komunikasi dengan konfigurasi tersebut. Untuk dapat melakukan akses ke 10.2.2.2, dapat digunakan password vpnpa55.



Konfigurasikan juga isakmp phase 2 pada R1, dengan membuat transform-set vpn-set untuk membuat esp-3des dan esp-sha-mac, dan membuat crypto map vpn-map. Dibuat vpn-map dengan name 10, agar vpn dapat terhubung. Lalu, definisikan IP dengan set peer, dan konfigurasi vpn dengan ipsec dengan transform-set. Setelah itu, tambahkan match address 110 untuk dapat menggunakan access list yang telah dibuat sebelumnya.



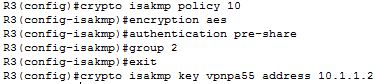
Pada interface s0/0/0, juga konfigurasikan crypto map. Langkah ini perlu dilakukan agar jelas interface mana yang akan digunakan untuk vpn.

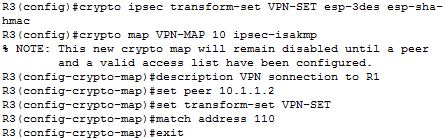
5.JPG

Selanjutnya, pada R3 konfigurasikan IPsec, dengan mengkonfigurasikan site-to-site VPN dengan R1 terlebih dahulu, dengan memberikan access-list seperti pada R1.

6.JPG

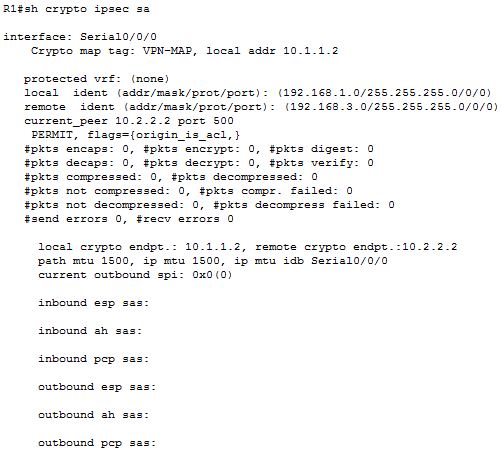
Kemudian, konfigurasikan R3 seperti R1, yaitu konfigurasikan isakmp phase 1, phase 2, dan crypto map pada interface.





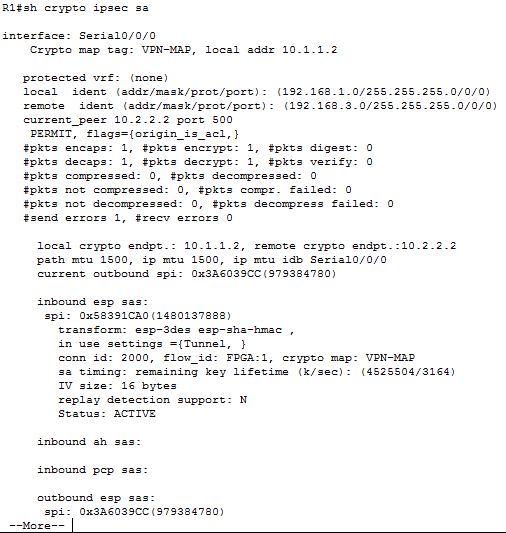
9.JPG

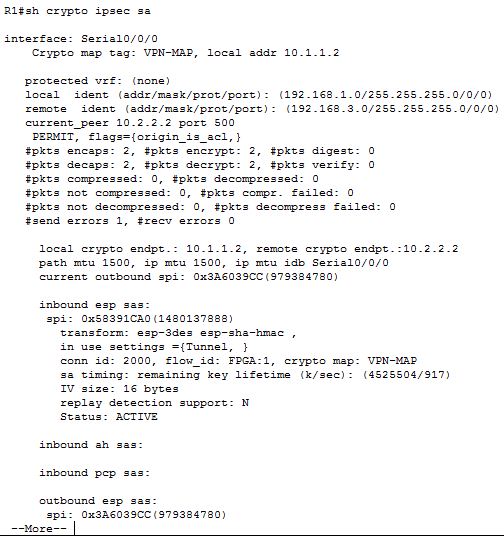
Lalu, lihat hasil konfigurasi pada R1, dengan show crypto ipsec sa.



Dan, coba lakukan ping dari PC-A ke PC-C, dan lihat lagi show crypto ipsec sa. Jika diperhatikan, maka setelah melakukan ping jumlah paket akan bertambah.

11.JPG





**Kesimpulan**

Pada VPN, dapat diterapkan IPsec untuk memberikan keamanan yang lebih pada jaringan, dan dengan menerapkan akses yang site-to-site, dan menggunakan kriptografi, autentikasi, dan key management protocol. IPsec adalah protokol yang dapat digunakan untuk meangamankan transmisi datagram dalam sebuah internetwork berbasis TCP/IP. IPsec melakukan enkripsi terhadap data pada lapisan yang sama dengan protokol IP dan menggunakan teknik tunneling untuk mengirimkan informasi melalui jaringan intermet atau dalam jaringan intranet secara aman. Untuk membuat sebuah sesi komunikasi yang aman dengan IPsec, maka dibutuhkan framework protokol yang disebut ISAKMP (Internet Security Association and Key Management Protocol). Framework tersebut mencakup beberapa algortima kriptografi yang telah ditentukan sebelumnya.