BAB 1

PENDAHULUAN

1.1. Latar Belakang

Dunia maya atau yang lebih kita kenal dengan *internet* merupakan dunia tanpa batas, segala hal apapun bisa kita cari dan dapatkan disana, tidak seperti jaman dahulu, *internet* yang masih sangat langka atau bisa dibilang adalah suatu barang mahal, namun sekarang *internet* bukan lagi barang mahal atau langka, sudah setiap orang bisa mendapatkan dengan mudah. Di dalam dunia tanpa batas tersebut bukan hanya hal positif yang bisa kita dapatkan, hal negatif juga bisa kita dapatkan tanpa sengaja, seperti *virus, malware, phising, sniffing*. Untuk itu, bagi para perusahaan besar atau menengah, bahkan perusahaan kecil, berusaha melindungi jaringan mereka masing-masing.

Alila Villas Uluwatu adalah salah satu hotel berbintang di daerah Bali, memiliki beberapa infrastruktur, salah satu infrastruktur dari hotel tersebut adalah jaringan, jaringan *LAN* dan jaringan *WAN*. Fungsi jaringan *LAN* pada hotel tersebut adalah sebagai penghubung antara satu divisi atau bagian dengan divisi lainnya, sedangkan fungsi jaringan *WAN* bukan hanya yang menghubungkan bagian *LAN* menuju area *internet* (*Wide Area Network*), tetapi juga sebagi salah satu fasilitas bagi seorang *Network engineer* yang bekerja disana untuk melakukan *maintenance* dan *monitoring*. Selain itu Alila juga mempunyai *web server* dan *mail server*, dimana kedua server tersebut harus dilindungi. Untuk membuat fasilitas tersebut dan melindungi kedua *server* tersebut, memerlukan peralatan yang lebih kompleks dan lebih aman, yang lebih handal, memiliki *throughput* yang besar, agar bagian dalam jaringan atau zona internal lebih aman, *router* bisa dikatakan kurang mampu untuk melakukan tugas ini, untuk itu digunakankanlah *firewall*.

Firewall adalah suatu sistem pertahanan terdepan pada suatu jaringan, sebagai peralatan yang memproteksi aliran data pada suatu jaringan. Alila Villas Uluwatu menggunakan *firewall Cisco Asa* 5510 atau 5500 *Series* sebagai *firewall* dalam jaringannya. Dengan fitur yang dimiliki oleh *Cisco Asa* seperti, *remote access*, *Intrusion Prevention*, *content Security*, *unified communications*, *botnets*, dan karena beberapa hal lain, maka Alila Villas Uluwatu memilih *Cisco Asa* 5510 atau 5500 *Series* sebagai *firewall*-nya, mengapa *Cisco* tidak seperti *open source* lain yang dipakai, karena *Cisco* adalah *firewall* yang handal, selain itu *firewall* yang dipilih haruslah memiliki *throughput* yang besar sesuai kebutuhan perusahaan, dimana banyak pengguna yang menggunakan jaringan tersebut. *After sales support* bagi *firewall* berbayar juga merupakan salah satu nilai tambah dalam memilih *firewall* 5510 ini, dan juga *firewall* ini dijadikan sebagai *VPN gateway*.

Namun seperti apa penggunaan *Cisco Asa* atau 5500 *Series* ini, apa saja yang harus diperhatikan dalam merancang suatu *firewall*, dan implementasinya. Secara keseluruhan, *firewall* memberikan fitur *NAT*, *Access list*, serta *VPN*, fitur *Access list* erat kaitannya dengan *NAT* pada *firewall*, dikarenakan *Cisco Asa Series* ini memiliki zona dengan prioritas tinggi dan zona dengan prioritas rendah yang berkaitan dengan *NAT* dan *Access list*.

Dimana dalam rangka penghematan *IP public*, dan kebutuhan akan keamanan, serta fleksibilitas dalam administrasi jaringan, *NAT* sangat efektif dalam mengatasi masalah tersebut. Alila Villas Uluwatu memiliki *Network engineer* yang tidak selalu berada di tempat, dengan kata lain, si *engineer* datang hanya jika diperlukan, dan *monitoring* harus tetap dilakukan untuk memantau aktifitas jaringan dalam hotel. Penambahan konfigurasi yang dilakukan oleh *engineer* dari tempat yang jauh yang tidak mungkin menjadi mungkin, memerlukan koneksi *VPN* ke dalam *firewall*.

Erat kaitannya *Access list* dengan *NAT*, membuat *Access list* perlu dikonfigurasikan dalam melakukan *NAT*, dimana secara *default* zona *trust*

yang berprioritas tinggi sebelum melakukan *NAT*, akan berimplisit *Access list*, dimana *firewall* akan mengizinkan *trust* untuk keluar dari area lokal, namun akan membaca *Access list* yang telah dibuat, meskipun secara *default* mempunyai *rule permit*.

Membatasi atau memblokir suatu *port* atau suatu "*session*" atau dengan kata lain *ICMP* dalam jaringan juga hal penting, karena dengan demikian orang-orang yang mencoba menembus pertahanan dari luar jaringan, dapat dicegah, karena dengan memblokir atau membatasi port atau "*session*" atau *ICMP*, keberadaan server dan peralatan utama jaringan dapat disembunyikan secara *virtual* untuk mencegah terjadinya hal yang tidak diinginkan.

1.2. Identifikasi Masalah

Berdasarkan latar belakang, penulis mengidentifikasikan masalah yang ditemukan, yaitu sebagai berikut :

1.2.1. Bagaimana merancang topologi jaringan hotel Alila Villas Uluwatu yang handal dari sisi keamanan dan infrastruktur?

1.2.2. Bagaimana hasil pengujian *NAT* dan *VPN* yang telah dikonfigurasi pada *firewall Cisco Asa*?

1.3. Tujuan Penulisan

Tujuan dari penulisan ini adalah sebagai berikut,

1.3.1. Memaparkan hasil rancangan topologi jaringan pada hotel Alila Villas Uluwatu.

1.3.2. Memaparkan hasil pengujian konfigurasi *NAT* dan *VPN* yang diterapkan pada *firewall Cisco Asa*, sebagai bahan uji coba bahwa konfigurasi telah dilakukan dengan benar.

1.4. Manfaat Penulisan.

Manfaat dari penulisan ini adalah,

1.4.1. Memaparkan suatu topologi, dan mengenalkan apa itu topologi jaringan.

1.4.2. Menjelaskan bagaimana melindungi suatu jaringan dan mengapa jaringan layak mendapatkan perlindungan.

1.4.3. Menjelaskan teori-teori *NAT* dan *VPN* bagi mereka yang belum mengenal atau belum tahu apa itu *NAT* dan *VPN*, dan apa fungsinya.