JAWABAN UJIAN AKHIR SEMESTER (UAS)

Dosen Pengampu :

Dr. Thoyyibah T., S.Kom., M.Kom

OLEH

ASEP RIDWAN HIDAYAT

231012050036

TI 01MKME001 REGULAR C

PROGRAM STUDI MAGISTER TEKNIK INFORMATIKA

UNIVERSITAS PAMULANG

TANGERANG SELATAN

2024

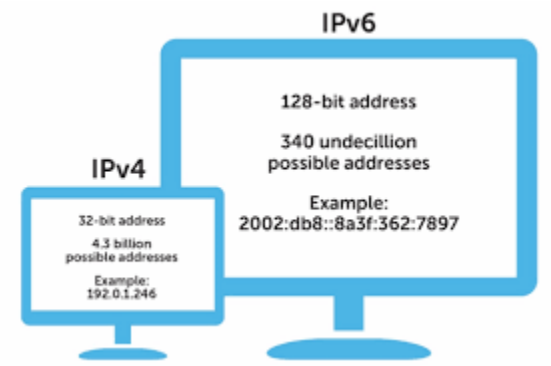
Soal :

1) Jelaskan perbedaan antara IPv4 dan IPv6. Mengapa IPv6 diperlukan meskipun IPv4 masih digunakan secara luas?
2) Diskusikan bagaimana firewall bekerja dalam melindungi jaringan komputer. Sebutkan dan jelaskan dua jenis firewall yang umum digunakan.
3) Apa itu Virtual Private Network (VPN) dan bagaimana teknologi ini meningkatkan keamanan komunikasi dalam jaringan?
4) Bagaimana protokol TCP/IP bekerja dalam mengirimkan data melalui jaringan? Jelaskan proses pengiriman data dari sumber ke tujuan.

1. Jawaban No. 1

A. Perbedaan Antara IPv4 Dan IPv6 Diantaranya Sebagai Berikut

Secara visual perbedaan antara IPv4 dan IPv6 seperti berikut



Gambar 1.1 Sumber : https://djppi.kominfo.go.id/news/kenapa-harus-beralih-ke-ipv6-apa-saja-keunggulannya-dibanding-ipv4

Fitur	IPv4	IPv6
Alamat IP	• Menggunakan alamat 32-bit yang terdiri dari empat kelompok angka desimal yang dipisahkan oleh titik (misalnya, 192.168.0.1). • Alamat IPv4 memiliki sekitar 4,3 miliar kombinasi unik.	• Menggunakan alamat 128-bit yang terdiri dari delapan kelompok angka heksadesimal yang dipisahkan oleh titik dua (misalnya, 2001:0db8:85a3:0000:0000:8a2e:0370:7334). • Alamat IPv6 memiliki sekitar 3,4 x 10^38 kombinasi unik.
Kapasitas Alamat	• Kapasitas alamat terbatas dan hampir habis karena pertumbuhan perangkat yang terhubung ke internet.	• Kapasitas alamat sangat besar, memungkinkan lebih banyak perangkat untuk terhubung tanpa kehabisan alamat.
Konfigurasi Otomatis	• Mendukung konfigurasi otomatis menggunakan protokol DHCP (Dynamic Host Configuration Protocol).	• Mendukung konfigurasi otomatis yang lebih canggih dengan stateless address autoconfiguration (SLAAC), yang memungkinkan perangkat untuk mendapatkan

		alamat IP tanpa memerlukan server DHCP.
Keamanan	• Keamanan biasanya diimplementasikan pada layer aplikasi, menggunakan protokol seperti IPSec (Internet Protocol Security) sebagai tambahan.	• IPSec adalah bagian integral dari protokol IPv6, memberikan keamanan end-to-end yang lebih baik secara native.
Header Paket	• Header paket lebih kompleks dengan beberapa field opsional	• Header paket lebih sederhana dengan lebih sedikit field, yang membantu meningkatkan efisiensi routing dan pengolahan paket
Fragmentasi	• Router di sepanjang jalur dapat melakukan fragmentasi paket.	• Hanya pengirim asli yang dapat melakukan fragmentasi; router tidak melakukan fragmentasi paket.
Kompatibilitas dan Implementasi	• Lebih luas digunakan saat ini karena merupakan versi protokol yang lebih tua dan lebih matang.	• Sedang dalam proses adopsi, namun penggunaannya semakin meningkat seiring dengan kebutuhan akan lebih banyak alamat IP.

B. IPv6 diperlukan meskipun IPv4 masih digunakan secara luas karena beberapa alasan berikut:

1) Pengambangan dari IPv4

- Secara garis besar IPv6 adalah pengembangan dari IPv4, juga IPv6 dioptimalkan untuk mengatasi keterbatasan yang ada pada IPv4 dan memenuhi kebutuhan internet masa depan. Dan beberapa hal lagi

2) Kekurangan Alamat IPv4

- Adanya kekurangan Alamat IPv4 yaitu Jumlah alamat IPv4 yang tersedia semakin menipis karena pertumbuhan internet yang pesat dan proliferasi perangkat yang terhubung. Hal ini menyebabkan kelangkaan alamat IPv4,

3) Keamanan

- IPv6 memiliki fitur keamanan bawaan yang lebih kuat daripada IPv4, seperti:

    a. IPsec (Internet Protocol Security): IPsec menyediakan enkripsi dan otentikasi data, sehingga lebih sulit bagi peretas untuk menyadap atau memodifikasi data.
    b. Alamat Stateless: IPv6 menggunakan alamat stateless, yang berarti alamat tidak secara permanen dikaitkan dengan perangkat. Hal ini membuat lebih sulit bagi peretas untuk melacak dan menargetkan perangkat.

4) Efisiensi Routing

IPv6 dirancang dengan struktur alamat yang hierarkis dan efisien, yang dapat meningkatkan efisiensi routing data di internet

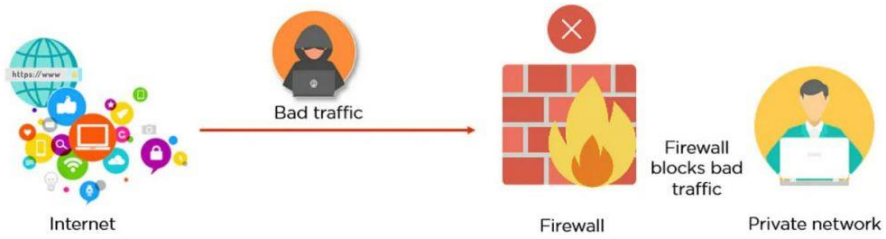
5) Dukungan untuk Jaringan Masa Depan

IPv6 diperlukan untuk mendukung jaringan masa depan seperti Internet of Things (IoT) dan 5G. Jaringan ini akan membutuhkan miliaran perangkat yang terhubung, dan IPv4 tidak memiliki kapasitas untuk menangani jumlah perangkat yang begitu banyak.

2. Jawaban No. 2

A. Berikut Adalah Cara Firewall Bekerja Dalam Melindungi Jaringan Komputer

Secara visual cara kerjanya seperti gambar berikut



Gambar 1.2 Sumber : https://www.niagahoster.co.id/blog/firewall-adalah/

Penjelasan lebihnya firewaal dalam melindungi jaringan computer diataranya berikut ini:

1. Pemeriksaan Paket (Packet Filtering)

- Firewall memeriksa header setiap paket data yang masuk atau keluar jaringan.
- Berdasarkan aturan yang telah ditentukan, firewall memutuskan apakah paket tersebut diizinkan masuk atau keluar dari jaringan.
- Aturan ini bisa berdasarkan alamat IP sumber atau tujuan, port yang digunakan, atau jenis protokol (TCP, UDP, ICMP, dll.).

2. Stateful Inspection

- Selain memeriksa header paket, stateful firewall juga melacak status koneksi yang ada.

- Firewall ini dapat menentukan apakah sebuah paket data adalah bagian dari koneksi yang sudah ada atau koneksi baru yang tidak diizinkan.
- Ini memberikan keamanan yang lebih karena dapat mengenali dan memblokir paket yang mencurigakan berdasarkan status koneksi.

3. Proxy Service:

   - Firewall proxy bertindak sebagai perantara antara perangkat dalam jaringan internal dan internet.
   - Semua permintaan akses internet dari jaringan internal diarahkan ke firewall proxy terlebih dahulu.
   - Firewall proxy kemudian meneruskan permintaan ini ke tujuan yang sebenarnya setelah memverifikasi keamanannya.
   - Data yang kembali dari internet juga melewati firewall proxy sebelum mencapai perangkat internal.

4. Deep Packet Inspection (DPI):

   - Firewall ini memeriksa data yang ada dalam payload paket, bukan hanya headernya.
   - DPI memungkinkan firewall untuk mengenali dan memblokir serangan yang lebih canggih, seperti malware dan eksploitasi aplikasi.
   - Ini memberikan tingkat keamanan yang lebih tinggi karena dapat mendeteksi pola serangan yang tersembunyi dalam data.

5. Network Address Translation (NAT)

   - Firewall menggunakan NAT untuk menyembunyikan alamat IP internal dari jaringan eksternal.
   - Ini membuat perangkat internal lebih sulit diidentifikasi dan diserang oleh pihak luar.
   - NAT juga membantu menghemat alamat IP publik dengan memungkinkan banyak perangkat menggunakan satu alamat IP publik.

6. Pengaturan Kebijakan Keamanan (Security Policies)

   - Firewall memungkinkan administrator jaringan untuk menetapkan kebijakan keamanan yang ketat.
   - Ini bisa mencakup pembatasan akses ke situs web tertentu, memblokir aplikasi tertentu, atau mengatur jam akses jaringan.
   - Kebijakan ini membantu mengendalikan aktivitas pengguna dan mencegah akses yang tidak sah atau berbahaya.

7. Pendeteksian dan Pencegahan Intrusi (IDS/IPS):

- Beberapa firewall memiliki fitur IDS/IPS yang dapat mendeteksi dan mencegah serangan jaringan secara real-time.
- IDS mengidentifikasi aktivitas mencurigakan atau serangan yang sedang terjadi.
- IPS tidak hanya mendeteksi tetapi juga memblokir serangan sebelum mencapai jaringan internal.

B. Dua firewall yang paling umum digunakan yaitu

1. Jaringan Firewall (Network Firewall)

- Pengertian Jaringan Firewall

Jaringan firewall adalah perangkat atau program yang mengontrol lalu lintas jaringan antara dua atau lebih jaringan. Firewall ini sering digunakan untuk melindungi jaringan internal dari ancaman eksternal, seperti internet.

- Jenis-Jenis Jaringan Firewall

a) Packet-Filtering Firewall: Firewall ini memeriksa header setiap paket data (alamat IP, port, protokol) dan menentukan apakah paket tersebut boleh lewat atau diblokir berdasarkan aturan yang telah ditetapkan.
b) Stateful Inspection Firewall: Firewall ini tidak hanya memeriksa header paket tetapi juga melacak status koneksi jaringan (state). Ini memungkinkan firewall untuk membuat keputusan lebih baik tentang apakah suatu paket merupakan bagian dari koneksi yang sah atau tidak.
c) Proxy Firewall: Firewall ini bertindak sebagai perantara antara pengguna internal dan sumber daya eksternal. Permintaan dari pengguna internal diteruskan melalui firewall proxy, yang kemudian meneruskan permintaan ke tujuan sebenarnya setelah memverifikasi keamanannya.

- Kelebihan

a) Dapat mengendalikan akses berdasarkan alamat IP dan port.
b) Mampu melindungi jaringan internal dari serangan yang berasal dari luar.
c) Stateful inspection dapat memberikan keamanan yang lebih baik dibandingkan dengan packet filtering.

- Kekurangan:

a) Tidak efektif dalam menganalisis isi paket (payload) untuk mendeteksi ancaman yang lebih kompleks.
b) Bisa menjadi titik kegagalan tunggal jika tidak dirancang dengan redundansi yang memadai.

2. Firewall Aplikasi (Application Firewall)

- Pengertian:

Firewall aplikasi adalah jenis firewall yang memantau dan mengendalikan lalu lintas jaringan ke atau dari aplikasi tertentu. Firewall ini bekerja pada lapisan aplikasi (layer 7 dalam model OSI), sehingga dapat menganalisis data yang lebih rinci daripada firewall jaringan.

- Jenis-Jenis:

a) Web Application Firewall (WAF): Firewall ini khusus digunakan untuk melindungi aplikasi web. WAF dapat mendeteksi dan mencegah serangan yang menargetkan kerentanan dalam aplikasi web, seperti SQL injection, cross-site scripting (XSS), dan lainnya.
b) Database Firewall: Firewall ini digunakan untuk melindungi basis data dari akses yang tidak sah dan serangan. Firewall ini memantau lalu lintas antara aplikasi dan database dan dapat mencegah serangan seperti SQL injection.

- Kelebihan:

a) Mampu menganalisis isi paket (payload) untuk mendeteksi ancaman yang lebih kompleks dan spesifik terhadap aplikasi.
b) Dapat melindungi aplikasi dari berbagai jenis serangan yang menargetkan kerentanan spesifik aplikasi.
c) Memungkinkan penerapan kebijakan keamanan yang lebih rinci dan spesifik untuk setiap aplikasi.

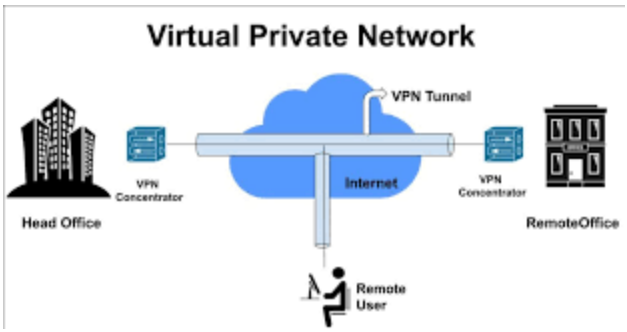
- Kekurangan:

a) Biasanya lebih kompleks dan membutuhkan konfigurasi yang lebih rumit dibandingkan firewall jaringan.
b) Mungkin memerlukan sumber daya lebih banyak (CPU, memori) untuk menganalisis dan memproses lalu lintas aplikasi.
c) Biasanya fokus pada aplikasi tertentu, sehingga mungkin tidak memberikan perlindungan menyeluruh terhadap semua jenis lalu lintas jaringan.

3. Jawaban No. 3

A. Pengertian Virtual Private Network

Secara visual vpn seperti dibawah ini



Gambar 1.3 Sumber : https://onlinelearning.uhamka.ac.id/login/index.php

Virtual Private Network (VPN) adalah layanan yang menciptakan koneksi aman dan terenkripsi antara perangkat dengan internet. Ini berfungsi seperti terowongan yang menyembunyikan aktivitas dan lokasi online dari pengintaian.

Berikut beberapa poin penting mengenai VPN

- Enkripsi Data: VPN mengenkripsi data yang dikirim dan diterima sehingga tidak dapat dibaca oleh pihak ketiga seperti peretas, penyedia layanan internet, atau bahkan pemerintah
- Anonimitas Online: Dengan menggunakan VPN, alamat IP asli pengguna disembunyikan dan digantikan dengan alamat IP dari server VPN. Ini membantu melindungi identitas online pengguna.
- Akses Konten Terbatas: VPN memungkinkan pengguna untuk mengakses konten yang mungkin diblokir atau dibatasi di wilayah tertentu, seperti layanan streaming atau situs web tertentu.
- Keamanan Koneksi: VPN membantu melindungi koneksi internet saat menggunakan jaringan Wi-Fi publik, yang biasanya kurang aman dan rentan terhadap serangan.

B. Cara) meningkatkan keamanan VPN dalam jaringan

Teknologi VPN (Virtual Private Network) meningkatkan keamanan komunikasi dalam jaringan dengan beberapa cara:

1) Enkripsi Data

VPN mengenkripsi data yang dikirim dan diterima menggunakan algoritma enkripsi yang kuat. Enkripsi ini memastikan bahwa data tidak dapat dibaca oleh pihak ketiga yang tidak berwenang. Bahkan jika data tersebut diintersepsi, enkripsi membuatnya tidak dapat dipahami tanpa kunci dekripsi yang benar.

2) Tunneling:

VPN menciptakan "terowongan" aman antara perangkat pengguna dan server VPN. Data yang melewati terowongan ini dilindungi dari pengintai dan peretas. Protokol tunneling seperti OpenVPN, L2TP/IPSec, dan SSTP memastikan bahwa data tetap aman saat transit.

3) Penyembunyian Alamat IP:

VPN menyembunyikan alamat IP asli pengguna dan menggantinya dengan alamat IP dari server VPN. Ini membantu melindungi identitas online pengguna dan membuatnya lebih sulit bagi pihak ketiga untuk melacak aktivitas online mereka.

Keamanan Jaringan Publik:

VPN melindungi data saat pengguna terhubung ke jaringan Wi-Fi publik, yang sering kali kurang aman. Dengan VPN, data yang dikirim dan diterima di jaringan publik dienkripsi, sehingga mengurangi risiko peretasan dan pencurian data.

4) Autentikasi:

VPN menggunakan metode autentikasi yang kuat untuk memastikan bahwa hanya pengguna yang sah yang dapat mengakses jaringan VPN. Metode autentikasi ini dapat mencakup penggunaan kata sandi, sertifikat digital, atau token keamanan.

5) Integritas Data:

VPN memastikan integritas data melalui mekanisme seperti checksum dan hash. Ini memastikan bahwa data tidak diubah atau dimanipulasi selama transmisi.

6) Perlindungan terhadap Serangan:

VPN dapat melindungi pengguna dari berbagai jenis serangan siber seperti Man-in-the-Middle (MitM), di mana penyerang mencoba mencegat dan mengubah komunikasi antara dua pihak yang berkomunikasi.

7) Kebijakan Tanpa Log:

Banyak penyedia VPN menerapkan kebijakan tanpa log, yang berarti mereka tidak menyimpan catatan aktivitas pengguna. Ini meningkatkan privasi dan mengurangi risiko data pengguna diekspos.

4. Jawaban No.4

A. Cara TCP/IP bekerja dalam mengirimkan data melalui jaringan

Berikut adalah penjelasan tentang bagaimana TCP/IP bekerja dalam mengirimkan data melalui jaringan:

1) Protokol Internet (IP):
   - IP bertanggung jawab untuk mengarahkan paket data dari sumber ke tujuan melalui jaringan yang terdiri dari berbagai perangkat dan jalur. IP menggunakan alamat IP untuk mengidentifikasi perangkat di jaringan.
   - Fragmentasi dan Reassembly: Jika paket data terlalu besar untuk dikirim dalam satu segmen, IP memecahnya menjadi fragmen yang lebih kecil. Setiap fragmen dikirim secara terpisah dan kemudian disatukan kembali di tujuan.

- Alamat IP: Setiap perangkat di jaringan memiliki alamat IP unik. IPv4 menggunakan alamat 32-bit (misalnya, 192.168.1.1), sementara IPv6 menggunakan alamat 128-bit (misalnya, 2001:0db8:85a3:0000:0000:8a2e:0370:7334).

2) Protokol Kontrol Transmisi (TCP):
   - TCP bertanggung jawab untuk memastikan bahwa data dikirimkan dengan andal dan dalam urutan yang benar. TCP menyediakan mekanisme kontrol aliran, pengurutan paket, dan koreksi kesalahan.

   - Three-Way Handshake: Sebelum data dikirim, TCP menginisiasi koneksi dengan proses tiga langkah (SYN, SYN-ACK, ACK) untuk memastikan bahwa kedua perangkat siap berkomunikasi.
   - Segmentation: Data dibagi menjadi segmen-segmen kecil yang lebih mudah diatur dan dikirimkan.
   - Nomor Urut dan Acknowledgement: Setiap segmen diberi nomor urut, dan penerima mengirimkan tanda terima (acknowledgement) untuk segmen yang diterima. Jika segmen hilang atau rusak, pengirim akan mengirim ulang segmen tersebut.
   - Kontrol Aliran: TCP mengatur laju pengiriman data untuk menghindari kelebihan beban di jaringan atau pada perangkat penerima.
3) Proses Pengiriman Data:
   - Encapsulation: Data dari aplikasi (misalnya, email, web browser) dikemas dalam segmen TCP, yang kemudian dibungkus dalam paket IP.
   - Routing: Paket IP dikirimkan melalui jaringan, melewati beberapa router yang mengarahkan paket berdasarkan alamat IP tujuan. Setiap router memeriksa header IP untuk menentukan jalur terbaik ke tujuan.
   - Decapsulation: Saat paket IP mencapai tujuan, lapisan IP menghapus header IP dan meneruskan segmen TCP ke lapisan TCP.
   - Reassembly: TCP di perangkat tujuan mengurutkan kembali segmen-segmen yang diterima berdasarkan nomor urut dan merakitnya menjadi data asli. Jika ada segmen yang hilang, TCP akan meminta pengirim untuk mengirim ulang segmen tersebut.
   - Pengiriman ke Aplikasi: Setelah semua segmen dikumpulkan dan diurutkan, data dikirim ke aplikasi tujuan (misalnya, aplikasi email, web browser) untuk diproses.

4) Keandalan dan Kontrol Kesalahan:

   TCP menggunakan beberapa mekanisme untuk memastikan keandalan pengiriman data:

   - Checksum: Setiap segmen TCP memiliki checksum untuk mendeteksi kesalahan selama transmisi. Jika segmen rusak, penerima akan membuang segmen tersebut dan meminta pengirim untuk mengirim ulang.
   - Retransmission: Jika pengirim tidak menerima tanda terima (acknowledgement) dalam waktu tertentu, segmen yang hilang akan dikirim ulang.

- Pengurutan Ulang: Segmen-segmen yang diterima di luar urutan akan diurutkan kembali sebelum diteruskan ke aplikasi.

5) Protokol Lain dalam Suite TCP/IP:

   Selain TCP dan IP, suite TCP/IP juga mencakup protokol lain seperti:

   - UDP (User Datagram Protocol): Protokol yang lebih sederhana dan cepat dibandingkan TCP, tetapi tanpa keandalan dan pengurutan. Digunakan untuk aplikasi yang membutuhkan kecepatan tinggi dan toleransi terhadap kehilangan data, seperti streaming video.
   - ICMP (Internet Control Message Protocol): Digunakan untuk mengirim pesan kesalahan dan informasi operasional di jaringan (misalnya, ping).
   - ARP (Address Resolution Protocol): Digunakan untuk memetakan alamat IP ke alamat MAC (Media Access Control) pada jaringan lokal.

B. Penjelasan Proses pengiriman data dari sumber ke tujuan dalam jaringan

Berikut adalah langkah-langkah pengiriman data dari sumber tujuan:

1) Aplikasi (Application Layer)
   Data dihasilkan oleh aplikasi (misalnya, email, browser web).
2) Transport (Transport Layer)
   Data dari aplikasi dibagi menjadi segmen oleh protokol transport seperti TCP atau UDP
3) TCP (Transmission Control Protocol)
   - Establish Connection: Koneksi diinisiasi dengan proses tiga langkah (SYN, SYN-ACK, ACK).
   - Segmentation: Data dibagi menjadi segmen-segmen kecil.
   - Numbering and Acknowledgement: Segmen diberi nomor urut dan dikirim. Penerima mengirim tanda terima (ACK) untuk segmen yang diterima.
   - Error Detection and Retransmission: Jika segmen hilang atau rusak, TCP akan meminta pengirim untuk mengirim ulang.
4) UDP (User Datagram Protocol)
   - Segmen dari transport layer dibungkus dalam paket IP.
   - Alamat IP: Paket IP diberi alamat IP sumber dan tujuan.
   - Routing: Paket diarahkan melalui jaringan oleh router berdasarkan alamat IP tujuan.
5) Internet (Network Layer)
   - Paket IP dibungkus dalam frame yang sesuai dengan protokol lapisan link (misalnya, Ethernet, Wi-Fi).
   - Alamat MAC: Frame diberi alamat MAC sumber dan tujuan.
   - Media Access: Frame dikirim melalui media fisik (kabel, gelombang radio).

Untuk Proses Pengiriman Data secara garis berasnya seperti berikut:

- Encapsulation (Pengemasan Data)
- Transmission (Pengiriman)
- Routing (Pengarahan)
- Decapsulation (Pembongkaran Data)
- Delivery (Pengiriman ke Aplikasi)