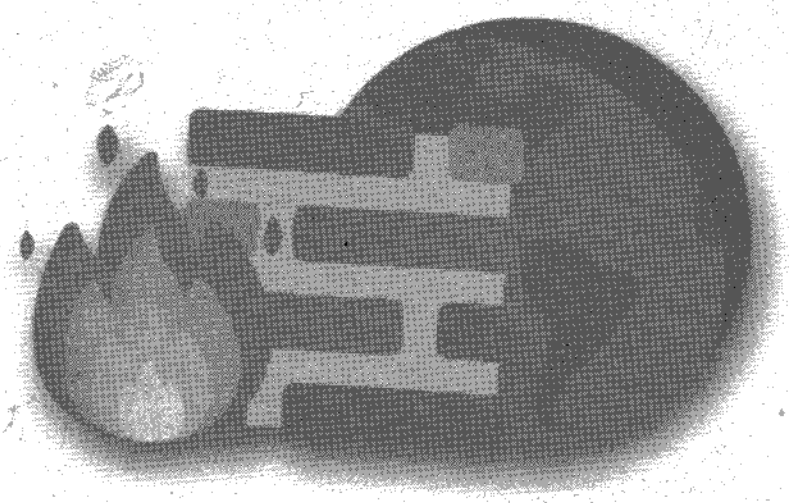
BAB V *Firewall* pada Jaringan VoIP

Bacalah teks berikut dengan saksama!



Sumber: *http://ghorizahal.nusahost.net/index.php/2018/10/01/konfigurasi-firewall-pada-debian-8/, diakses 14 Desember 2018 , 15.13 WIB*

Gambar 5.1 *Firewall* dalam jaringan VoIP

Di era perkembangan internet yang semakin canggih, setiap komputer dapat terhubung dengan komputer lainnya secara mudah. Begitu pula dengan teknologi telepon berbasis IP. Pertukaran komunikasi, *file*, atau dokumen pun semakin tanpa batas dan dapat dilakukan oleh siapa saja. Tentunya hal ini membawa dampak positif, namun selain itu juga memiliki dampak negatif.

Dampak positifnya yaitu pengguna akan semakin dimudahkan dalam berkomunikasi dan berbagi data. Sementara itu dampak negatifnya, tidak semua orang berbagi dengan tujuan baik. Beberapa berusaha untuk menyerang jaringan, memata-matai (*spoinase*) sambungan komunikasi tertentu demi kepentingan pribadi, menyadap, dan lain sebagainya.

Untuk mencegah dampak negatif tersebut, dibutuhkan *firewall* sebagai pengatur sistem komunikasi antara dua buah jaringan. *Firewall* dapat didefinisikan sebagai proses yang didesain spesifik untuk menahan akses yang ingin masuk ke dalam jaringan pribadi. *Firewall* dapat berwujud perangat lunak ataupun perangkat keras, atau dapat juga dari kombinasi keduanya.

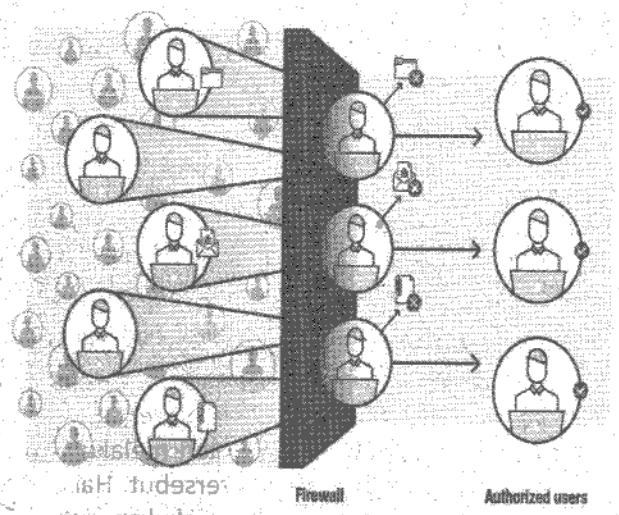
Agar dapat berfungsi secara efektif, sebuah *firewall* wajib memenuhi standar tertentu, mampu mendirikan suatu 'pagar pengaman' di sekeliling sebuah jaringan komunikasi pribadi, mencegah masuknya akses tanpa izin dan berbagai gangguan terhadap dokumen atau *file* yang berada pada sisi pengguna.

A. Mengenal Pengertian dan Peran *Firewall*

Dalam membangun sebuah *server softswitch* ataupun jaringan komunikasi lainnya, perlu memperhatikan tingkat keamanan pada jaringan tersebut. Keamanan jaringan pengguna perlu diidentifikasi, hal ini untuk mencegah penyusup yang ingin masuk dan mengakses setiap bagian dari sistem jaringan komunikasi. Kemanan jaringan komunikasi tersebut salah satunya dapat dengan menerapkan *firewall*. Untuk mengetahui apa itu *firewall* dan fungsi *firewall* pada jaringan VoIP, pelajari materi berikut dengan sungguh-sungguh!

1. Pengertian *Firewall* dalam Jaringan

Firewall adalah sebuah sistem atau perangkat yang memberikan otorisasi pada lalu lintas jaringan komputer ataupun komunikasi yang dianggapnya aman untuk melaluinya dan melakukan pencegahan terhadap jaringan yang dianggap tidak aman. Perlindungan dengan menggunakan *firewall* sangat penting untuk komputasi perangkat seperti komputer *server* yang diaktifkan dengan koneksi internet. *Firewall* sangat diperlukan karena bertindak sebagai gerbang keamanan antara jaringan komputer internal dan jaringan komputer eksternal.



Sumber: *https://www.trendmicro.com/, diakses 15 Desember 2018 , 09.44 WIB*

Gambar 5.2 Mengenal *firewall* dalam jaringan

Dalam jaringan komputer, khususnya yang berkaitan dengan aplikasi yang melibatkan berbagai kepentingan, akan banyak terjadi hal yang dapat mengganggu kestabilan koneksi jaringan komputer tersebut, baik yang berhubungan dengan *hardware*, *software*, *human error*, maupun disebabkan oleh pihak ketiga. Gangguan yang disebabkan oleh pihak ketiga ini biasanya berupa perusakan, penyusupan, pencurian hak akses, penyalahgunaan data maupun sistem, hingga tindakan *cyber crime*.

2. Fungsi *Firewall* dalam Jaringan

Firewall didesain untuk mengizinkan *private* data, menolak layanan yang mudah diserang, serta mencegah jaringan internal dari serangan luar yang dapat menembus *firewall* setiap waktu. Di dalam jaringan, *firewall* memiliki fungsi di antaranya yaitu:

a. Mengontrol serta mengawasi arus paket data yang mengalir pada jaringan.
b. Mengatur, memfilter, dan mengontrol lalu lintas data yang diizinkan untuk mengakses jaringan *private*. Terdapat beberapa kriteria untuk mengontrol lalu lintas data, yaitu:
    1) IP *address* dari komputer sumber.
    2) *Port* TCP/UDP sumber dari sumber.
    3) IP *address* dari komputer tujuan.
    4) *Port* TCP/UDP tujuan data pada komputer tujuan.
    5) Informasi dari *header* yang disimpan dalam paket data.
c. Melakukan autentifikasi terhadap akses.
d. Mencatat semua kejadian yang terdapat pada jaringan.
e. Mampu memeriksa *header* dari paket data.

Secara spesifik fungsi *firewall* yaitu melakukan autentifikasi terhadap akses ke jaringan. Agar semakin memperjelas pemahamanmu mengenai fungsi *firewall*, berikut adalah penjelasan dari beberapa fungsi *firewall*.

a. Mengontrol dan Mengawasi Paket Data yang Terdapat pada Jaringan

Firewall secara teknis merupakan sebuah program yang memiliki fungsi untama untuk melakukan proses pengamanan dan pengontrolan dari paket data yang masuk dan juga yang

mengalir di dalam setiap jaringan komputer. Apabila *firewall* pada sebuah jaringan diaktifkan, maka *firewall* akan menyeleksi dan juga memilah-milah paket data yang akan diakses. Hal ini akan membantu *firewall* dalam meneruskan konten yang aman dan konten yang tidak aman bagi komputer ataupun jaringan komunikasi.

Dengan kemampuan mengontrol dan juga menyeleksi, program *firewall* memiliki kontribusi yang tinggi terhadap pemblokiran dari konten-konten yang dapat membahayakan. Selain itu *firewall* dapat pula bertindak sebagai antivirus yang cukup membantu. Peranan ini erat hubungannya dengan fungsi *routing table* pada *router* yang bertugas untuk membuka jalur paket yang disalurkan ke seluruh *client*.

b. Melakukan Proses Autentifikasi terhadap Akses dalam Jaringan

Dengan adanya *firewall* dapat berfungsi untuk meningkatkan keamanan jaringan melalui proses autentifikasi. Proses autentifikasi ini merupakan proses di mana pengguna harus memberikan *password* yang sudah diatur sebelumnya di dalam sebuah sistem agar pengguna dapat menggunakan suatu jaringan. Apabila proses autentifikasi gagal, maka jaringan tersebut akan menutup dan tidak dapat diakses. Oleh karena itu, dari segi keamanan penggunaan *firewall* sangat efektif sebagai benteng pertahanan suatu jaringan dari penggunaan yang tidak bertanggung jawab. Terdapat beberapa mekanisme autentikasi yang dapat digunakan yaitu: *Firewall* dapat meminta input dari pengguna mengenai nama pengguna (*user name*) serta kata kunci (*password*), mekanisme kedua adalah dengan menggunakan sertifikat digital dan kunci publik, dan mekanisme selanjutnya dengan menggunakan *Pre-Shared Key* (PSK) atau kunci yang telah diberitahu kepada pengguna.

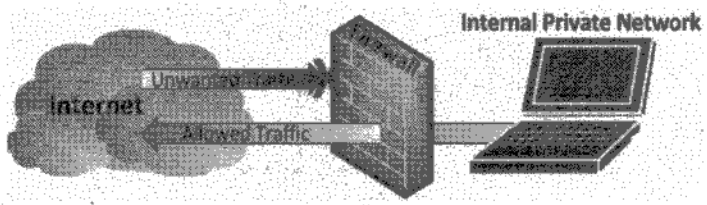
c. Melakukan Recording dari Setiap Arus Transaksi pada Satu Sesi

Firewall memiliki fungsi teknis selain mengontrol paket data dan melakukan proses autentifikasi, yaitu sebagai *recorder* atau melakukan pencatatan. Fungsi sebagai *recorder* ini maksudnya adalah *firewall* akan melakukan proses *recording* dari setiap transaksi yang sudah dilakukan di dalam jaringan tersebut. Hal ini berarti, *firewall* akan merekam dan juga mencatat setiap aktivitas internet yang dilakukan oleh pengguna di dalam sebuah jaringan. Untuk kemudian membantu mendeskripsikan konten apa saja yang biasanya diakses oleh pengguna tersebut di dalam sebuah jaringan.

Kegiatan 5.1

A. Judul Kegiatan : Menganalisis Konsep *Firewall* dalam Jaringan
B. Jenis Kegiatan : Diskusi Kelompok
C. Tujuan Kegiatan :
1) Peserta didik dapat menjelaskan mengenai konsep *firewall* dalam jaringan dengan benar. (KD 3)
2) Peserta didik dapat mengilustrasikan konsep *firewall* dengan terampil. (KD 4)

D. Langkah Kegiatan :
1. Buatlah kelompok yang beranggotakan 3-4 orang dan tunjuklah salah seorang sebagai ketua!
   Ketua Kelompok : .....
   Anggota 1 : .....
   Anggota 2 : .....
   Anggota 3 : .....
2. Perhatikan gambar berikut dengan saksama!



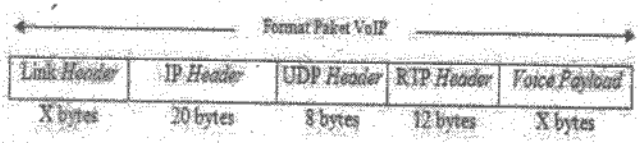
Sumber: *https://www.tunnelsup.com/what-is-a-firewall/, diakses 15 Desember 2018, 11.26 WIB*

Gambar 5.3 Ilustrasi *firewall* dalam jaringan

3. Berdasarkan gambar ilustrasi di atas, bersama kelompokmu lakukanlah analisis terhadap pengertian dan konsep *firewall* sesuai dengan pemahaman kalian!
   Hasil analisis:
   .....
   .....
4. Bersama kelompokmu jelaskan mengenai peran *firewall* dalam suatu jaringan!
   Peran *firewall* dalam jaringan:
   .....
   .....
5. Berdasarkan hasil analisis yang telah kalian lakukan, ilustrasikan/demonstrasikan konsep *firewall* dalam jaringan di depan kelas. Kalian dapat menggunakan alat bantu dengan barang-barang yang berada di sekitarmu!
6. Mintalah tanggapan dari guru dan kelompok lain!
   Tanggapan:
   .....
   .....

Permasalahan dan Penyelesaian

Permasalahan 5.1:
Hal yang paling penting dalam membangun sebuah jaringan VoIP adalah mengetahui struktur jaringan tersebut. Ini bertujuan agar *Administrator* memahami sehingga dapat menerapkan sistem keamanan yang tepat pada jaringan, khususnya adalah *firewall*. Bagaimana struktur dan format paket VoIP?
Penyelesaian:
Secara umum, tiap paket VoIP terdiri dari dua bagian, yakni *header* dan *payload* (beban/informasi). *Header* terdiri dari: IP *header*, *Real-Time Transport Protocol* (RTP) *header*, *User Datagram Protocol* (UDP) *header* dan *data link header*. Format paket VoIP ditunjukkan pada gambar berikut:



Sumber: *https://www.kajianpustaka.com/2012/10/voip-voice-over-internet-protocol.html, diakses 17 Desember 2018, 08.43 WIB*

Gambar 5.4 Struktur dan format paket VoIP

1. IP *header* : bertugas menyimpan informasi routing untuk mengirimkan paket-paket ke tujuan. Pada tiap *header* IP disertakan tipe layanan atau ToS (*Type of Service*) yang memungkinkan paket tertentu seperti paket suara diperlakukan berbeda dengan paket yang *non real time*.
2. UDP *header* memiliki ciri tertentu yang tidak menjamin paket akan menuju tujuan sehingga UDP cocok digunakan pada aplikasi *voice real time* yang sangat peka terhadap *delay/latency*.
3. RTP *header*, *header* yang dapat dimanfaatkan untuk melakukan *framing* dan segmentasi data *real time*, RTP juga tidak mendukung reabilitas paket untuk sampai ditujuan. RTP menggunakan protokol kendali RTCP (*Real Time Control Protocol*) yang mengendalikan QoS dan sinkronisasi media *stream* yang berbeda.
4. *Link header*, biasanya tergantung pada media yang digunakan. (PPP=6 *byte*).
5. *Voice Payload* menurut Cisco dan berdasarkan *Codec* yang digunakan (G.723,1 dengan 5,3 Kbps) nilainya 20 *Bytes*.

Sumber: *https://www.kajianpustaka.com/2012/10/voip-voice-over-internet-protocol.html, diakses 17 Desember 2018, 08.43 WIB*

Bagaimana pendapatmu (minimal 15 kata) : .....
.....
.....

Apa alasannya (minimal 30 kata) : .....
.....
.....

Permasalahan 5.2:

Firewall merupakan perangkat dengan suatu cara atau metode yang digunakan untuk melindungi sistem, baik itu sistem komputer ataupun sistem jaringan yang lebih luas, dalam hal ini termasuk jaringan komunikasi VoIP. *Firewall* berfungsi untuk memonitor paket data yang masuk dan keluar dari jaringan. Dalam penggunaannya terdapat jenis *firewall* yang bersifat stateful. Bagaimana cara *firewall* tersebut bekerja?

Penyelesaian:

Firewall bersifat stateful, hal ini berarti *firewall* akan mengingat koneksi yang melaluinya sehingga dapat mengizinkan lalu lintas kembali untuk aliran yang sama. Jika *firewall* diatur untuk memblokir semua lalu lintas yang masuk tetapi mengizinkan semua lalu lintas yang keluar. *Firewall* stateful akan melacak permintaan apa yang berbasal dari dalam sehingga berfungsi untuk mengizinkan ketika lalu lintas kembali dari luar menuju ke jaringan lokal. Hal ini berfungsi pada saat setiap lalu lintas diminta kembali untuk menuju ke jaringan lokal oleh mesin di bagian dalam jaringan.

Sumber: *https://www.tunnelsup.com/what-is-a-firewall/, diakses 17 Desember 2018, 09.15 WIB.*

Bagaimana pendapatmu (minimal 15 kata) : .....
.....
.....

Apa alasannya (minimal 30 kata) : .....
.....
.....

3. Cara Kerja *Firewall* dalam Jaringan

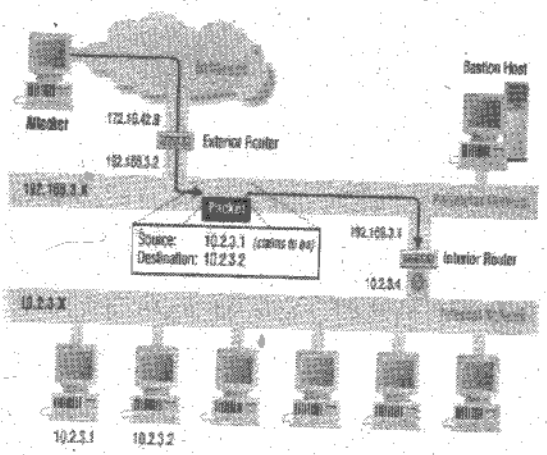
Firewall bekerja dengan cara membatasi akses jaringan pribadi dengan internet. *Firewall* bekerja seperti penjaga keamanan di depan gerbang rumah dan mengidentifikasi pengunjung yang datang, serta menyaring penyusup yang berusaha memasuki jaringan pribadi. *Firewall* bertugas untuk menahan segala usaha *hacking* yang masuk ke dalam jaringan pribadi. Secara umum, *firewall* memiliki beberapa cara kerja, di antaranya:

a. *Firewall* menutup *traffic* yang datang (*incoming network traffic*) berdasarkan sumber atau tujuan dari *traffic* tersebut. *Firewall* akan memblok *incoming network traffic* yang tidak diinginkan adalah fitur yang paling umum yang disediakan oleh *firewall*.
b. *Firewall* menutup *traffic* yang keluar (*outgoing network traffic*) berdasarkan sumber atau tujuan dari *traffic* tersebut. *Firewall* juga bisa menyaring *traffic* yang yang berasal dari jaringan internal ke internet, misalnya ketika kita ingin mencegah *user* dari mengakses situs-situs yang tidak diperbolehkan.
c. *Firewall* menutup *traffic* berdasarkan kontennya. *Firewall* yang lebih canggih dapat memonitor *traffic* dari konten-konten yang tidak diinginkan, misalnya *firewall* yang di dalamnya terintegrasi antivirus ia dapat mencegah *file* yang terinveksi oleh virus masuk ke komputer atau jaringan komputer internal yang kita miliki.
d. *Firewall* melaporkan *traffic* di jaringan dan kegiatan *firewall*. Ketika memonitor *traffic* jaringan dari dan ke Internet, yang juga penting adalah mengetahui apa yang dikerjakan oleh *firewall*, siapa yang mencoba membobol jaringan internal dan siapa yang mencoba mengakses informasi yang tidak layak dari Internet.

Teknologi *firewall* semakin hari semakin berkembang. Sebelumnya, *firewall* bekerja menyaring lalu lintas komputer dengan menggunakan alamat IP, nomor *port*, serta protokol. Seiring dengan perkembangannya, *firewall* kini mampu menyaring data yang masuk dengan mengidentifikasi terlebih dahulu pesan konten yang dibawanya. Untuk mengatur lalu lintas perpindahan data jaringan pribadi dan internet, *firewall* dapat menggunakan salah satu atau gabungan dari beberapa metode berikut ini:

a. *Packet filtering*

Merupakan sebuah cara kerja *firewall* dengan memonitor paket yang masuk dan keluar, mengizinkan paket tersebut untuk lewat atau tertahan berdasarkan alamat IP, protokol, dan *port*. *Packet filtering* biasanya cukup efektif digunakan untuk menahan serangan dari luar sebuah LAN. *Packet filtering* disebut juga dengan *firewall* statis. Selama terjadinya komunikasi dengan jaringan internet, paket yang datang disaring dan dicocokkan dengan aturan yang sebelumnya telah dibuat dalam membangun *firewall*. Jika data tersebut cocok, maka data dapat diterima dan sebaliknya jika tidak cocok dengan aturan, maka data tersebut ditolak.



Sumber: *https://docstore.mik.ua/orelly/networking_2ndEd/fire/ch08_01.htm, diakses 20 Desember 2018, 11.13 WIB*

Gambar 5.5 Metode *packet filtering*

Dalam metode *packet filtering*, *firewall* mengecek sumber dan tujuan alamat IP. Pengirim paket mungkin saja menggunakan aplikasi dan program yang berbeda, sehingga *packet filtering* juga mengecek sumber dan tujuan protokol, seperti UDP (*User Datagram Protocol*) dan TCP (*Transmission Control Protocol*).

b. ***Inspeksi Stateful***

Berkebalikan dengan *Packet filtering*, Inspeksi Stateful dikenal pula dengan *firewall* dinamis. Pada inspeksi stateful, status aktif koneksi dimonitor, kemudian info yang didapatkan akan dipakai untuk menentukan apakah sebuah paket jaringan dapat menembus *firewall*.

Inspeksi stateful secara besar-besaran telah menggantikan *packet filtering*. Pada *firewall* statis, hanya *header* dari paket yang diperiksa, artinya seorang hacker dapat mengambil informasi melalui *firewall* dengan sederhana, yaitu mengindikasikan "*reply*" melalui *header*. Sementara dengan *firewall* dinamis, sebuah *packet* dianalisis hingga ke dalam lapisan-lapisannya, dengan merekam alamat IP dan juga nomor *port*nya, sehingga keamanannya lebih ketat dibandingkan *packet filtering*.

4. Teknologi *Firewall* pada Jaringan Komputer

Terdapat beberapa macam teknologi yang terdapat pada *firewall*. Teknologi-teknologi tersebut antara lain adalah sebagai berikut.

a. *Service* ***Control (Kendali terhadap Layanan)***

Teknologi *firewall* berdasarkan tipe-tipe layanan yang digunakan di internet dan dapat diakses baik untuk ke dalam ataupun keluar *firewall*. Biasanya *firewall* akan memeriksa IP *address* dan juga nomor *port* yang digunakan baik pada protokol TCP dan UDP, bahkan *proxy* yang akan menerima dan menerjemahkan setiap permintaan akan suatu layanan sebelum mengizinkannya. Teknologi ini juga dapat menjadi perangkat lunak pada *server* itu sendiri, seperti layanan untuk web ataupun *mail*.

b. ***Direction Control (Kendali terhadap Arah)***

Teknologi ini berdasarkan arah dari berbagai permintaan (*request*) terhadap layanan yang akan dikenali dan diizinkan melewati *firewall*.

c. ***User Control (Kendali terhadap Pengguna)***

Teknologi ini berdasarkan pengguna/*user* yang berfungsi untuk dapat menjalankan suatu layanan. Hal ini berarti ada *user* yang dapat dan ada yang tidak dapat menjalankan suatu servis/layanan, yaitu dikarenakan *user* tersebut tidak diizinkan untuk melewati *firewall*. Teknologi ini biasanya digunakan untuk membatasi *user* dari jaringan lokal untuk mengakses keluar, tetapi bisa juga diterapkan untuk membatasi terhadap pengguna dari luar.

d. ***Behavior Control (Kendali terhadap Perlakuan)***

Teknologi ini berdasarkan seberapa banyak layanan itu telah digunakan. Misalnya, *firewall* dapat memfilter *email* untuk menanggulangi/mencegah *spam*.

Kegiatan 5.2

A. Judul Kegiatan : Memahami Cara Kerja *Firewall* dalam Jaringan

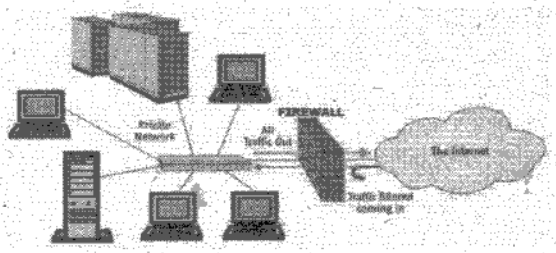
B. Jenis Kegiatan : Tugas Mandiri

C. Tujuan Kegiatan :

1) Peserta didik dapat menjelaskan mengenai cara kerja *firewall* dengan benar. (KD 3)
2) Peserta didik dapat menentukan cara kerja *firewall* yang baik pada jaringan di sekitarnya dengan terampil. (KD 4)

D. Langkah Kegiatan :

1. Perhatikan gambar berikut dengan saksama!



Sumber: *https://www.indiamart.com/proddetail/firewalls-8626428762.html, diakses 17 Desember 2018, 14.37 WIB*

Gambar 5.6 Skema cara kerja *firewall* dalam jaringan

2. Lakukanlah analisis mengenai cara kerja *firewall* yang kamu ketahui berdasarkan gambar di atas!
   Hasil analisis:
   .....
   .....
3. Berdasarkan hasil analisis di atas, berikan ilustrasi sederhana cara kerja *firewall* pada jaringan yang berada di sekitarmu. Deskripsikan secara rinci!
   Cara kerja *firewall* pada jaringan yang berada di sekitar:
   .....
   .....
4. Carilah informasi mengenai jenis-jenis *firewall* pada jaringan! Kamu dapat menggunakan buku, internet, dll sebagai bahan informasi! Jelaskan mengenai jenis-jenis *firewall* tersebut!
   jenis-jenis *firewall* pada jaringan:
   .....
   .....
5. Berdasarkan hasil analisis, ilustrasi, dan informasi yang telah kamu kerjakan, jelaskan apakah *firewall* jaringan yang berada di sekitarmu sudah bekerja dengan baik! Berikan pendapatmu!
   Pendapat:
   .....
   .....

Permasalahan dan Penyelesaian

Permasalahan 5.3:

Firewall dalam jaringan dapat berupa PC, *router*, *midrange*, *mainframe*, UNIX *workstation* atau gabungan dari keseluruhan komponen tersebut. *Firewall* dalam jaringan bertugas untuk memproteksi sebuah komputer dari segala macam serangan yang tidak diinginkan yang berpotensi untuk merusak, menyadap, atau bahkan melakukan akses remote terhadap komputer dalam sebuah jaringan. Terdapat beberapa karakteristik *firewall*. Apa saja karakteristik-karakteristik tersebut?

Penyelesaian:

Berikut merupakan karakteristik *firewall* jaringan, yaitu:

1. *Firewall* harus bisa lebih kuat dan kebal terhadap serangan eksternal/luar. Hal ini berarti sistem operasi komputer akan relatif lebih aman dan penggunaan sistemnya dapat dipercaya.
2. Hanya aktivitas yang dikenal atau terdaftar saja yang dapat melakukan hubungan. Dalam hal ini dilakukan dengan mengatur *policy setting* pada konfigurasi keamanan lokalnya.
3. Seluruh aktivitas yang berasal dari dalam ke luar harus melewati *firewall* terlebih dahulu. Hal ini dilakukan dengan membatasi maupun memblok setiap akses terhadap jaringan lokal, kecuali jika melewati *firewall* terlebih dahulu.

Sumber: *https://www.sekolahpendidikan.com/2017/09/pengertian-firewall-karakteristik.html#, diakses 17 Desember 2018, 14.45 WIB*

Bagaimana pendapatmu (minimal 15 kata) : .....

.....

.....

Apa alasannya (minimal 30 kata) : .....

.....

.....

Permasalahan 5.4:

Firewall merupakan sebuah program yang dikembangkan untuk meningkatkan proteksi dan keamanan komputer yang terhubung ke dalam jaringan tersebut. Dalam penerapannya, *firewall* memiliki keuntungan dan kelemahan. Apa keuntungan dan kelemahan menggunakan *firewall* dalam jaringan?

Penyelesaian:

Berikut adalah keuntungan menggunakan *firewall* dalam jaringan:

1. *Firewall* merupakan fokus dari segala keputusan sekuritas. Hal ini disebabkan karena *firewall* merupakan satu titik tempat keluar masuknya trafik internet pada suatu jaringan.
2. *Firewall* dapat menerapkan suatu kebijaksanaan sekuritas. Banyak sekali *service-service* yang digunakan di internet. Tidak semua *service* tersebut aman digunakan, oleh karenanya *firewall* dapat berfungsi sebagai penjaga untuk mengawasi *service-service* mana yang dapat digunakan untuk menuju dan meninggalkan suatu *network*.
3. *Firewall* dapat mencatat segala aktivitas yang berkaitan dngan alur data secara efisien. Semua trafik yang melalui *firewall* dapat diamati dan dicatat segala aktivitas yang berkenaan dengan alur data tersebut. Dengan demikian *Network Administrator* dapat segera mengetahui jika terdapat aktivitas-aktivitas yang berusaha untuk menyerang internal *network* mereka.
4. *Firewall* dapat digunakan untuk membatasi penggunaan sumber daya informasi. Mesin yang menggunakan *firewall* merupakan mesin yang terhubung pada beberapa *network* yang berbeda, sehingga kita dapat membatasi *network* mana saja yang dapat mengakses suatu *service* yang terdapat pada *network* lainnya.

Sementara kelemahan menggunakan *firewall* dalam jaringan adalah sebagai berikut:

1. *Firewall* tidak dapat melindungi *network* dari serangan koneksi yang tidak melewatinya (terdapat pintu lain menuju *network* tersebut).
2. *Firewall* tidak dapat melindungi dari serangan dengan metode baru yang belum dikenal oleh *firewall*.
3. *Firewall* tidak dapat melindungi dari serangan virus.

Bagaimana pendapatmu (minimal 15 kata) : .....

.....

.....

Apa alasannya (minimal 30 kata) : .....

.....

.....

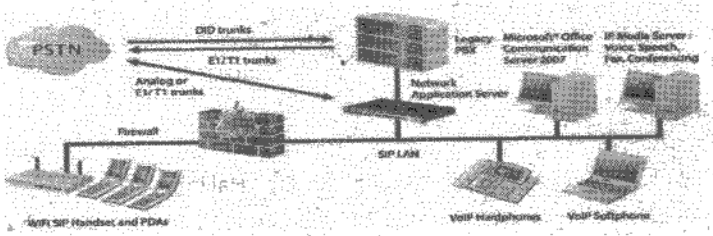
B. *Firewall* pada Jaringan VoIP

Jaringan VoIP merupakan jaringan yang menyediakan layanan aplikasi multimedia. Jaringan ini memiliki struktur yang cukup rumit dibandingkan dengan jaringan komputer, sehingga keamahan yang dimiliki pun harus lebih terjamin. Sistem keamanan salah satunya dapat menggunakan *firewall*. Untuk memperdalam pemahamanmu mengenai konsep dan fungsi *firewall* dalam jaringan VoIP, pelajari materi berikut dengan sungguh-sungguh!

1. Konsep *Firewall* pada Jaringan VoIP

Jaringan VoIP memiliki struktur yang cukup rumit jika dibandingkan dengan jaringan komputer. Karena itu maka mekanisme sekuritas terhadap serangan yang mengambil keuntungan dari kelemahan jaringan VoIP perlu dikembangkan. Hal ini bertujuan untuk menangkal ancaman dan serangan dengan mendefinisikan atau membentuk dengan proses yang baik. Sehingga pendekatan yang berlapis untuk mempertahankan kemanan pada jaringan VoIP dapat terjamin. Dalam pembangunannya, jaringan VoIP harus dirancang untuk menggabungkan kontrol yang dapat mengatasi hal-hal seperti berikut:

a. Mengidentifikasi ancaman yang berlaku,
b. Mengidentifikasi serangan dan meminimalkan peluang serangan,
c. Meminimalkan dampak dari serangan, dan
d. Mengelola dan mengurangi serangan secara tepat waktu.



Sumber: *http://www.nexcom.com.tw/applications/DetailByDivision/network-application-appliance, diakses 20 Desember 2018, 11.20 WIB*

Gambar 5.7 Konsep *firewall* pada jaringan VoIP

Pengembangan persyaratan keamanan di atas akan membantu untuk membangun arsitektur yang kuat dengan menggabungkan beberapa sistem keamanan dan ketersediaan QoS. Keamanan pada jaringan umumnya didefinisikan pada lima kategori sebagai berikut.

a. *Confidentiality*, kategori yang memberi persyaratan di mana informasi (data) hanya dapat diakses oleh pihak yang memiliki wewenang.
b. *Integrity*, kategori yang memberi persyaratan di mana informasi hanya dapat diubah oleh pihak yang memiliki wewenang.
c. *Availability*, kategori yang memberi persyaratan di mana informasi yang tersedia hanya untuk pihak yang memiliki wewenang ketika dibutuhkan.
d. *Authentication*, kategori yang menjelaskan bahwa pengirim suatu informasi dapat diidentifikasi dengan benar dan ada jaminan bahwa identitas yang didapat tidak palsu.
e. *Nonrepidiation*, kategori yang menjelaskan bahwa baik pengirim maupun penerima pesan informasi tidak dapat menyangkal pengiriman pesan.

2. Fungsi *Firewall* pada Jaringan VoIP

Internet merupakan sebuah jaringan yang sangat terbuka, konsekuensinya adalah tidak ada jaminan keamanan bagi jaringan yang terkait ke internet. Hal ini berarti apabila *Administrator* jaringan tidak berhati-hati dalam mengatur sistemnya, maka kemungkinan besar penyusup akan dengan mudah memasuki jaringan yang berhungan dengan internet. *Administrator* jaringan bertugas untuk menekan risiko tersebut seminimal mungkin. Fungsi *firewall* pada jaringan VoIP adalah mencegah gangguan pada sistem jaringan VoIP. Adapun 4 kategori bentuk gangguan pada sistem antara lain adalah sebagai berikut:

a. *Interruption*. Merupakan gangguan di mana suatu aset dari suatu sistem diserang sehingga tidak tersedia atau tidak dapat dipakai oleh yang berwenang. Contohnya perusakan/modifikasi terhadap piranti keras atau saluran jaringan.

b. *Interception*. Merupakan gangguan di mana pihak yang tidak berwenang mendapatkan akses pada suatu aset. Pihak yang dimaksud dapat berupa orang, program atau sistem yang lain. Contohnya penyadapan terhadap data dalam suatu jaringan.

c. *Modification*. Merupakan gangguan di mana pihak yang tidak berwenang tapi dapat melakukan perubahan terhadap suatu aset. Contohnya adalah perubahan nilai pada *file* data, modifikasi pesan yang sedang ditransmisikan dalam jaringan.

d. *Fabrication*. Merupakan gangguan di mana pihak yang tidak berwenang menyisipkan objek palsu ke dalam sistem. Contohnya adalah pengiriman pesan palsu kepada orang lain.

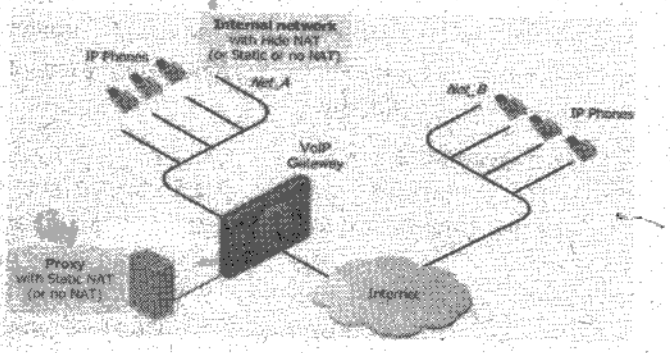
Firewall berfungsi sebagai *gateway* antara jaringan yang dilindunginya dengan jaringan lainnya. *Firewall* dirancang untuk mengendalikan aliran paket berdasarkan asal, tujuan, *port*, dan informasi tipe paket. *Firewall* berisi sederet daftar aturan yang digunakan untuk menentukan paket data yang melewati suatu jaringan. *Firewall* tersusun dari aturan-aturan yang diterapkan baik terhadap *hardware*, *software*, ataupun sistem itu sendiri dengan tujuan untuk melindungi jaringan dengan melakukan filterisasi, membatasi, ataupun menolak suatu permintaan koneksi dari jaringan luar lainnya. Berdasarkan kategori gangguan dan cara kerja *firewall* di atas, fungsi *firewall* dalam jaringan VoIP adalah sebagai berikut:

a. VoIP memiliki ribuan *port* yang dapat diakses untuk berbagai keperluan.
b. *Firewall* bertugas untuk menutup *port-port* tersebut kecuali beberapa *port* yang perlu tetap terbuka.
c. *Firewall* pada VoIP bertindak sebagai garis pertahanan pertama dalam mencegah semua jenis *hacking* atau penyusupan.
d. Menjaga informasi rahasia dan berharga agar tidak keluar tanpa diketahui oleh pengguna.
e. Untuk memodifikasi paket data yang datang melalui *firewall*.

Kegiatan 5.3

A. Judul Kegiatan : Menganalisis Konsep *Firewall* pada Jaringan VoIP
B. Jenis Kegiatan : Tugas Kelompok
C. Tujuan Kegiatan :
1) Peserta didik dapat menjelaskan mengenai konsep *firewall* pada jaringan VoIP dengan benar. (KD 3)
2) Peserta didik dapat membuat gambaran konsep *firewall* pada jaringan VoIP yang akan dibangun dengan terampil. (KD 4)

D. Langkah Kegiatan :
1. Buatlah kelompok yang beranggotakan 3-4 orang dan tunjuklah salah seorang sebagai ketua!
   Ketua Kelompok : .....
   Anggota 1 : .....
   Anggota 2 : .....
   Anggota 3 : .....
2. Perhatikan gambar berikut dengan saksama!



Sumber: *http://officialpackersjersey.com/, diakses 18 Desember 2018, 13.59 WIB*
Gambar 5.8 *Firewall* dalam jaringan VoIP

3. Berdasarkan gambar di atas, lakukanlah analisis terhadap konsep *firewall* pada jaringan VoIP!

Hasil analisis:

.....

.....

4. Berdasarkan hasil analisis yang telah kalian lakukan, buatlah skema jaringan VoIP yang akan kalian bangun dengan menerapkan *firewall*! Tulislah konsep *firewall* pada jaringan VoIP tersebut secara rinci!

Skema jaringan VoIP dengan *firewall*:

Konsep *firewall* pada jaringan VoIP:

.....

.....

5. Presentasikan hasilnya di depan kelas! Mintalah tanggapan dari guru dan kelompok lain!

Permasalahan dan Penyelesaian

Permasalahan 5.5:

Firewall dalam jaringan VoIP digunakan untuk mencegah gangguan penyusup atau *hacker* yang ingin memasuki jaringan VoIP tertentu. Dalam *internetworking* terdapat beberapa gangguan yang dapat terjadi. Apa saja gangguan-gangguan tersebut?

Penyelesaian:

Dalam *internetworking* dikenal ada beberapa istilah gangguan yaitu :

1. *Hacking*, berupa pengrusakan pada infrastruktur jaringan yang sudah ada, misalnya pengrusakan pada sistem dari suatu *server*.
2. *Physing*, berupa pemalsuan terhadap data resmi dilakukan untuk hal berkaitan dengan pemanfaatannya.
3. *Deface*, perubahan terhadap tampilan suatu *website* secara illegal.
4. *Carding*, pencurian data terhadap identitas perbankan seseorang, misalnya pencurian nomor kartu kredit.

Sumber: *https://slideplayer.info/slide/3107592/, diakses 18 Desember 2018, 15.10 WIB.*

Bagaimana pendapatmu (minimal 15 kata) : .....

.....

.....

Apa alasannya (minimal 30 kata) : .....

.....

.....

Permasalahan 5.6:

Keamanan dalam jaringan komunikasi tentunya menjadi poin penting. Hal ini bertujuan untuk mencegah adanya peretas atau penyusup yang ingin masuk ke dalam jaringan. Bagaimana cara melakukan persiapan pada saat membangun sebuah jaringan agar memiliki sistem pengamanan yang tepat?

Penyelesaian:

Berikut adalah hal-hal yang perlu dilakukan untuk membangun suatu jaringan agar memiliki sistem pengamanan yang baik:

1. Memisahkan terminal yang difungsikan sebagai pengendali jaringan atau titik pusat akses (*server*) pada suatu area yang digunakan untuk aplikasi tertentu.
2. Menyediakan pengamanan fisik berupa ruangan khusus untuk pengamanan perangkat yang disebutkan di atas. Ruangan tersebut dapat diberikan label *Network Operating Center* (NOC) dengan membatasi personel yang diperbolehkan masuk.
3. Memisahkan sumber daya listrik untuk NOC dari pemakaian yang lain. Hal ini untuk menjaga kestabilan fungsi sistem. Perlu juga difungsikan *Uninterupable Power Supply* (UPS) dan *stablizier* untuk menjaga kestabilan *suply* listrik yang diperlukan perangkat pada NOC.
4. Merapikan *wiring* ruangan dan memberikan label serta pengklasifikasian kabel.
5. Memberikan *soft security* berupa sistem *firewall* pada perangkat yang difungsikan di jaringan.
6. Merencanakan *maintenance* dan menyiapkan *backup* sistem.

Sumber: *http://www.academia.edu/22129370/Pengertian_SIP, diakses 6 Desember 2018, 14.55 WIB*

Bagaimana pendapatmu (minimal 15 kata) :
.....
.....

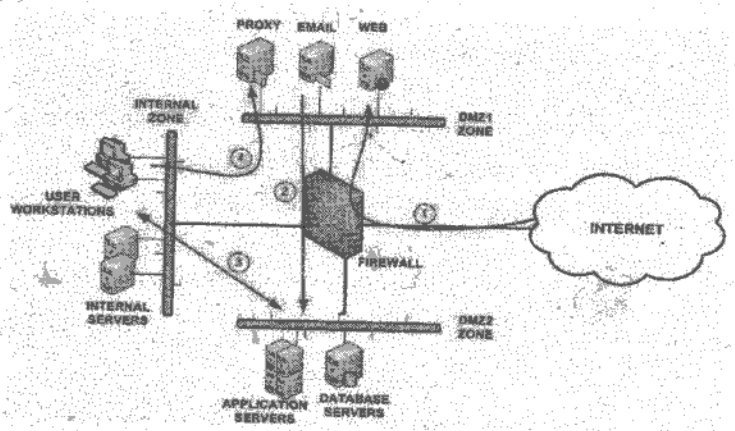
Apa alasannya (minimal 30 kata) :
.....
.....

3. Arsitektur *Firewall* pada Jaringan VoIP

Umumnya keamanan jaringan VoIP yang ditinjau dari arsitekturnya mencakup segmentasi jaringan yang tepat, arsitektur tersebut di antaranya yaitu:

a. *Network Segmentation*

Subnet mask/segmentasi jaringan berfungsi untuk mengetahui kelompok dari suatu IP. Arsitektur ini digunakan saat dibutuhkan suatu *rouing* atau pengalihan data antarkomputer, di mana perangkat *router* atau komputernya akan memeriksa apakah IP tujuan berada di kelompok/ *network* yang sama.

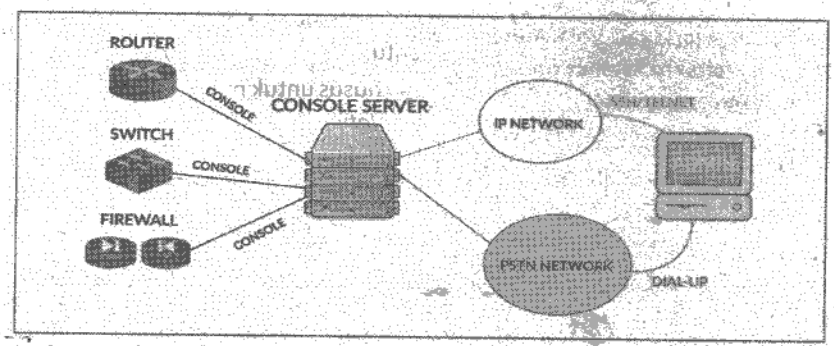


Sumber: *https://www.spamtitan.com/web-filtering/network-segmentation-best-practices/, diakses 11 April 2019, 14.43 WIB*

Gambar 5.9 Arsitektur *network segmentation*

b. *Out of band Network Management*

Konfigurasi secara *out of band* adalah dengan cara menghubungkan komputer secara langsung dengan *port console* atau dengan *port auxiliary* (AUX) dari *router* yang akan dikonfigurasikan. Jenis koneksi ini tidak memerlukan koneksi jaringan dari *router* tersebut. Teknisi jaringan menggunakan arsitektur *out of band* untuk konfigurasi awal, karena *router* tidak akan dapat berfungsi pada jaringan apabila tidak dikonfigurasikan terlebih dahulu. Arsitektur secara *out of band* juga digunakan ketika koneksi jaringan tidak berfungsi dengan benar sehingga *router* tidak dapat diakses melalui jaringan. Dalam membangun jaringan dengan menggunakan arsitektur *out of band* diperlukan *software* terminal *emulation client* yang ter*install* pada PC.



Sumber: *https://www.rahisystems.com/rahi-partner/out-of-band-management-whats-old-is-new-again/, diakses 19 Desember 2018, 10.13 WIB*

Gambar 5.10 Arsitektur *out of band*

c. Private Addressing

Private addressing digunakan sebagai mekanisme atau arsitektur lain untuk melindungi terhadap serangan eksternal. Pertumbuhan eksponensial dari internet di awal 1990-an mengakibatkan menipisnya alamat IP secara global. RFC 1918 mempublikasikan IETF dalam upaya untuk mendorong organisasi agar menggunakan alamat IP *nonroutable* untuk sistem yang tidak dimaksudkan untuk langsung terhubung ke internet. Dengan demikian dapat mencegah menipisnya alamat IP *routable*-internet.

4. Langkah-Langkah Membangun *Firewall* pada Jaringan VoIP

Dalam membangun *firewall* pada jaringan VoIP, berikut adalah langkah-langkah yang diperlukan:

a. Menentukan topologi jaringan VoIP yang akan digunakan. Nantinya topologi dan konfigurasi jaringan VoIP akan menentukan bagaimana *firewall* akan dibangun.

b. Menentukan kebijakan atau *policy* yang akan digunakan. Kebijakan yang dimaksud adalah penentuan aturan-aturan yang akan diberlakukan.

c. Menentukan aplikasi-aplikasi dan layanan-layanan apa saja yang akan berjalan di dalam jaringan VoIP. Aplikasi dan layanan yang akan berjalan harus diketahui oleh teknisi agar dapat menentukan aturan-aturan yang lebih spesifik pada *firewall* di dalam jaringan VoIP.

d. Menentukan pengguna mana saja yang akan dikenakan oleh satu atau lebih aturan *firewall*.

e. Menerapkan kebijakan, aturan, dan prosedur dalam implementasi *firewall*.

f. Mensosialisasikan kebijakan, aturan, dan prosedur yang sudah diterapkan. Lakukan pembatasan sosialisasi hanya kepada personil teknis yang diperlukan saja.

Kegiatan 5.4

A. Judul Kegiatan : Menerapkan Arsitektur *Firewall* pada Jaringan VoIP

B. Jenis Kegiatan : Tugas Kelompok

C. Tujuan Kegiatan :

1) Peserta didik dapat menjelaskan mengenai arsitektur *firewall* pada jaringan VoIP dengan benar. (KD 3)

2) Peserta didik dapat menentukan arsitektur *firewall* yang ingin digunakan pada jaringan VoIP dengan terampil. (KD 4)

D. Langkah Kegiatan :

1. Buatlah kelompok yang beranggotakan 3-4 orang dan tunjuklah salah seorang sebagai ketua!

Ketua Kelompok : .....

Anggota 1 : .....

Anggota 2 : .....

Anggota 3 : .....

2. *Firewall* pada jaringan VoIP memiliki beberapa arsitektur yang dapat diterapkan. Carilah artikel mengenai arsitektur-arsitektur tesebut dan tentukan poin-poin pentingnya!
   Poin-poin penting artikel:
   a. .....
   b. .....
   c. .....
   ... .

3. Berdasarkan artikel di atas, tentukan kelebihan dan kekurangan masing-masing arsitektur *firewall*!
   Kelebihan:
   .....
   .....

   Kekurangan:
   .....
   .....

4. Bersama kelompokmu, pilihlah salah satu arsitektur *firewall* yang ingin kalian gunakan pada jaringan VoIP yang akan kalian bangun!
   Arsitektur *firewall* yang ingin digunakan:
   .....
   Alasan penggunaan arsitektur:
   .....
   .....

5. Presentasikan hasil diskusi yang telah kalian lakukan di depan kelas! Mintalah tanggapan dari guru dan kelompok lain!

Permasalahan dan Penyelesaian

Permasalahan 5.7:
Firewall merupakan sebuah program yang berperan sebagai *network gateways* yang dapat melindungi *private network* dari *network* lain. Tentunya banyak sekali perubahan di dalam dunia IT terkait dengan semakin banyaknya aplikasi yang digunakan. Untuk mengimbangi perubahan-perubahan tersebut, maka telah dibuat *firewall* generasi baru atau yang dikenal dengan *Next Generation Firewall* (NGFW). Apa yang dimaksud dengan *next generation firewall*?

Penyelesaian:
Next generation firewall adalah kelas *firewall* yang diimplementasikan dalam perangkat lunak atau perangkat keras dan mampu mendeteksi dan memblokir serangan dengan tingkat kerumitan tinggi dengan menegakkan langkah-langkah keamanan di tingkat protokol, *port*, dan aplikasi. Perbedaan antara *firewall* standar dan *firewall* generasi berikutnya adalah yang terakhir melakukan pemeriksaan yang lebih mendalam dan dengan cara yang lebih cerdas. *Firewall* generasi mendatang juga menyediakan fitur tambahan seperti dukungan integrasi direktori aktif, inspeksi SSH dan SSL, dan penyaringan *malware* berdasarkan reputasi.

Sumber: *https://www.techopedia.com/definition/30649/next-generation-firewalls, diakses 19 Desember 2018, 11.26 WIB.*

Bagaimana pendapatmu (minimal 15 kata) : .....
.....
.....

Apa alasannya (minimal 30 kata) : .....
.....
.....

Permasalahan 5.8:

Firewall dibutuhkan untuk melindungi integritas data atau sistem jaringan dari serangan-serangan pihak yang tidak bertanggung jawab. *Firewall* melindungi jaringan lokal dengan cara mengendalikan aliran paket yang melewatinya. Pada *firewall* terjadi beberapa proses yang memungkinkannya melindungi jaringan. Apa saja proses tersebut?

Penyelesaian:

Ada beberapa macam proses yang terjadi pada *firewall* dalam melindungi jaringan, yaitu:

1. Modifikasi *header* paket, digunakan untuk memodifikasi kualitas layanan bit paket TCP sebelum mengalami proses *routing*.
2. Translasi alamat jaringan, translasi yang terjadi dapat berupa translasi satu ke satu (*one to one*), yaitu satu alamat IP *private* dipetakan ke satu alamat IP publik, atau translasi banyak ke satu (*many to one*) yaitu beberapa alamat IP *private* dipetakan ke satu alamat publik.
3. Filter paket, digunakan untuk menentukan nasib paket, apakah dapat diteruskan atau tidak.

Sumber: *https://www.slideshare.net/ekostereo/sistem-keamanan-jaringan-firewall, diakses 19 Desember 2018, 13.31 WIB.*

Bagaimana pendapatmu (minimal 15 kata) : .....

.....

.....

Apa alasannya (minimal 30 kata) : .....

.....

.....

HOTS (High Order Thinking Skills)

A. Pilihlah satu jawaban yang paling benar dengan cara memberi tanda silang (X) pada huruf *A, B, C, D,* atau *E* serta tuliskan alasannya!

1. Jaringan VoIP merupakan jaringan dengan struktur yang cukup rumit. Sehingga keamanan yang dimiliki pun harus lebih terjamin. Perlindungan dengan menggunakan *firewall* sangat penting untuk komputasi perangkat seperti komputer *server* yang diaktifkan dengan koneksi internet. Hal ini sebab ....
   A. *firewall* memiliki komponen-komponen yang dapat mencegah segala kemungkinan serangan pada jaringan.
   B. *firewall* bekerja pada *port* IEEE
   C. *firewall* didesain untuk mengizinkan *trusted* data, menolak layanan yang mudah diserang, serta mencegah jaringan internal dari serangan luar.
   D. *firewall* dapat mencegah adanya human error sehingga dapat memperkecil tingkat serangan pada jaringan.
   E. *firewall* tidak harus melakukan pengaturan *policy setting* sehingga lebih aman pada jaringan VoIP.

   Alasan: .....

   .....

2. Banyaknya perusahaan, kantor pemerintahan, dan sekolah yang memiliki akses ke internet, disarankan untuk melindungi aset digitalnya dari serangan *hacker*. Terlebih saat ini instansi-instansi tersebut memanfaatkan internet untuk membuat jaringan VoIP. Penggunaan *firewall* menjadi salah satu upaya yang dapat dilakukan. Kemampuan minimal yang harus dimiliki oleh *firewall* yaitu ....
   A. *firewall* harus menggunakan standar protokol IEEE
   B. *firewall* harus memiliki layanan yang dapat mengatasi masalah *malware*
   C. *firewall* menggunakan arsitektur DMZ
   D. *firewall* menggunakan iptables sebagai aplikasinya
   E. *firewall* harus bisa lebih kuat dan kebal terhadap serangan eksternal/luar

   Alasan: .....

   .....

3. *Firewall* pada jaringan VoIP bertujuan untuk menangkal ancaman dan serangan. Pengembangan persyaratan keamanan yang teoar akan membantu untuk membangun arsitektur yang kuat dengan menggabungkan beberapa sisemn keamanan. Sebuah sistem VoIP harus memiliki kemampuan *availability*. Hal ini karena ....

A. Jaringan VoIP harus mampu menjaga datanya agar dapat menyangkal pengiriman pesan.
B. jaringan VoIP harus dapat memberi persyaratan di mana informasi yang tersedia hanya untuk pihak yang memiliki wewenang.
C. jaringan VoIP harus mampu mengidentifikas serangan dan meminimalkan peluang serangan.
D. jaingan VoIP harus menjelaskan bahwa pengirim suatu informasi dapat diidentifikasi dengan benar dan ada jaminan bahwa identitad yang didapat tidak palsu.
E. VoIP merupakan layanan yang dibuat dengan *call processing language* yang memiliki kemampuan *find-me/follow-me*.

Alasan: .....
.....

4. Seorang teknisi sedang membangun sebuah jaringan VoIP di salah satu perusahaan pertambangan. Selanjutnya teknisi melakukan pengonfigurasian *firewall* terlebih dahulu. Arsitektur *firewall* yang mungkin digunakan oleh teknisi tersebut yaitu ....

A. *Network segmentation*
B. *Private addressing*
C. *Inspeksi stateful*
D. *Out of band*
E. *Packet filtering*

Alasan: .....
.....

5. Saat ini penggunaan jaringan komputer begitu pesat. Hampir seluruh instansi memanfaatkan internet di dalam jaringannya. Sehingga sangat penting untuk menjamin tingkat keamanannya. Dalam hal ini *firewall* memiliki peran yang sangat penting, hal ini karena ....

A. *Firewall* berfungsi mengatur, memfilter, dan mengontrol lalu lintas data yang diizinkan untuk mengakses jaringan *private*
B. *Firewall* merupakan jenis *security* jaringan yang memiliki tingkat keamanan yang tinggi
C. *Firewall* merupakan *security* jaringan yang menggunakan standar ITU-T tentang perencanaan jaringan
D. *Firewall* merupakan *security* jaringan yang dapat digunakan pada segala jenis *hardware* dan sistem operasi
E. *Firewall* dapat mencegah segala macam serangan *cyber crime*

Alasan: .....
.....

B. Jawablah pertanyaan berikut dengan tepat!

1. Jelaskan konsep *firewall* menurut pemahamanmu!
Jawaban: .....
.....

2. Gambar dan jelaskan cara kerja *firewall* berdasarkan pemahamanmu!
Jawaban: .....
.....

3. Jelaskan jenis serangan yang dapat sangat mengancam jaringan VoIP. Berikan alasannya secara rinci!
Jawaban: .....
.....

4. Jelaskan pentingnya keamanan pada jaringan VoIP!
Jawaban: .....
.....

5. Jelaskan peran *firewall* dalam sebuah jaringan VoIP!
Jawaban: .....
.....

Studi Kasus

I. Bacalah uraian berikut dengan sungguh-sungguh!

Apa itu *Firewall*?

Firewall adalah perangkat fisik atau perangkat lunak yang memberikan lapisan keamanan ke jaringan atau komputer. Tugas utamanya adalah hanya mengizinkan lalu lintas yang diperlukan untuk melewati dan memblokir semua lalu lintas lainnya.

Di jaringan lokal, lalu lintas tidak berasal dari internet menuju ke jaringan lokal. Namun, lalu lintas berasal dari dalam jaringan lokal yang menuju ke internet. *Firewall* dapat digunakan untuk memblokir semua lalu lintas masuk dan mengizinkan semua lalu lintas keluar. Ini akan memblokir banyak upaya dari peretas yang mencoba masuk ke jaringan lokal.

Firewall dapat diinstal sebagai program perangkat lunak pada satu komputer. Jenis *firewall* ini sering terbatas hanya memblokir lalu lintas masuk atau keluar dari komputer. Misalnya dalam sistem operasi *Windows*, *firewall* diinstal secara default. Ini akan memblokir lalu lintas yang masuk ke komputer tetapi memungkinkan lalu lintas yang keluar dari komputer.

Ada tiga alasan penting untuk menggunakan *firewall* pada jaringan: yaitu digunakan sebagai kontrol akses, NAT, dan VPN. Kontrol akses adalah tempat kebijakan dibuat untuk memblokir atau mengizinkan lalu lintas berdasarkan alamat IP, *port*, dan protokol. NAT, atau terjemahan alamat jaringan, adalah tindakan mengonversi satu alamat IP ke yang lain. *Firewall* sering dilengkapi untuk melakukan banyak jenis NAT yang akan menerjemahkan alamat IP internal pribadi ke alamat IP yang dapat diakses publik. *Firewall* juga sering memiliki kemampuan VPN. Jaringan Pribadi Virtual adalah teknologi yang digunakan untuk menghubungkan dua jaringan secara aman melalui jaringan tidak aman seperti internet.

.....

Sumber: *https://www.tunnelsup.com/what-is-a-firewall/, diakses 17 Desember 2018, 08.57 WIB.*

Untuk memperdalam pemahamanmu mengenai *firewall*, berlatihlah untuk melakukan analisis mengenai konsep kerja *firewall* dan pentinganya pada VoIP berdasarkan uraian di atas dengan menggunakan model pembelajaran *Discovery Learning*. Lengkapi tugas berikut sesuai dengan tahapan dibawah ini!

A. Rumusan Masalah

1. .....
2. .....

B. Kajian Pustaka yang Relevan

Guna menganalisis teks di atas, maka dibutuhkan kajian pustaka yang relevan yakni:

1. Kajian Pustaka I
   Sumber referensi: ..... (Tahun .....)
   Isi teori:
   .....
   .....
2. Kajian Pustaka II
   Sumber referensi: ..... (Tahun .....)
   Isi teori:
   .....
   .....

C. Data yang Diperoleh Peserta Didik

1. .....
2. .....
3. .....

D. Analisis Data

1. .....
2. .....
3. .....
4. .....
5. .....

E. Simpulan

.....

.....

II. Cermati dan pahamilah uraian berikut!

Keamanan Sistem pada Jaringan VoIP

VoIP menggunakan jaringan IP (*public network*) untuk transmisi data suara, dengan terlebih dahulu dilakukan kompresi sesuai standar VoIP ITU-T. Perancangan jaringan VoIP lebih menekankan masalah *delay* dan *bandwidth*. *Delay* didefiniskan sebagai waktu yang dibutuhkan untuk mengirimkan data dari sumber (pengirim) ke tujuan (penerima), sedangkan *bandwidth* adalah kecepatan maksimum yang dapat digunakan untuk melakukan transmisi data antarkomputer pada jaringan IP atau internet. Dengan VoIP, *bandwith* dalam transmisi data suara jadi berkurang. Karena bandwith data suara sebesar 64 Kbps (lewat *line* telepon) dikompresi menjadi 6 Kbps (untuk *half-duplex communication*). Sehingga biaya yang dikeluarkan menjadi lebih murah.

VoIP memanfaatkan jaringan IP (sebagai jaringan publik) dalam prosesnya. Jaringan publik sangat rawan terhadap *attackers*, karena jaringan publik digunakan oleh banyak pihak. Jaringan publik lebih rawan terhadap *attackers* dibandingkan dengan jaringan privat. Semua titik pada jaringan IP rawan terhadap *attackers*, terutama di *router*-nya. Data yang mengalir di luar jaringan IP juga rawan terhadap *attackers*.

.....

Sumber: *https://openlibrary.telkomuniversity.ac.id/pustaka/files/93889/resume/keamanan-sistem-pada-jaringan-voip-menggunakan-algoritma-kriptografi-seal-security-system-on-voip-network-using-seal-cryptographic-algorithm-.pdf, diakses 19 Desember 2018, 13.46 WIB.*

Berdasarkan uraian di atas, lakukanlah analisis untuk menentukan solusi terhadap permasalahan tersebut dengan menggunakan model pembelajaran *Problem Based Learning* dengan melengkapi tugas berikut sesuai dengan tahapan yang telah ditentukan!

A. Rumusan Masalah/Identifikasi Masalah/Pertanyaan Masalah

1. .....
2. .....
3. .....
4. .....
5. .....

B. Aktivitas/Kegiatan Belajar untuk Mengatasi/Menyelesaikan Masalah

No.	Aktivitas Pembelajaran Penyelesaian Masalah	Hasil yang Dicapai
1.	Diskusi Kelompok	Simpulan Diskusi: 1. ..... 2. ..... 3. ..... 4. .....
2.	Referensi yang Relevan	Hasil Referensi yang relevan: 1. ..... 2. ..... 3. ..... 4. .....

C. Analisis Data

.....

.....

D. Simpulan Solusi Masalah secara Kelompok

.....

.....

III. Cermati dan pahamilah uraian berikut!

Analisis Aspek Keamanan VoIP pada *Next Generation Network*

Jaringan Telco (PSTN/ISDN dan PLMN) yang berbasis *circuit switched* dengan elemen utamanya sentral telepon, memiliki banyak keterbatasan baik dari segi arsitektur maupun efisiensi pemakaian *resources* (*bandwidth*). Dari segi arsitekturnya elemen kontrol, elemen media dan aplikasinya bersifat *propietary* (*vendor dependent*) sehingga disamping relatif mahal, juga sulit dikembangkan. Dari segi pemakaian kanal *bandwidth*, karena koneksinya bersifat *dedicated* yang bersifat TDM (*Time Division Multiplexing*), utilitas kanal rendah yang berarti kurang efisien. Di sisi lain jaringan IP, protokolnya yang bersifat *open system* dan mode paket *switch* yang lebih efisien, membuatnya jaringan IP mampu berkembang lebih pesat, semakin mendominasi, bahkan mulai mengambil alih peran PSTN/ISDN bahkan PLMN atau selular.

Sekarang ini komunikasi multimedia sudah menjadi hal yang tidak dapat dipisahkan lagi dalam aplikasi internet. Aplikasi ini meliputi *Voice over Internet Protocol* (VoIP), konferensi multimedia, *Instant Messaging*, dan sebagainya. Oleh karena itu sangat dibutuhkan adanya suatu manajemen dalam pertukaran data yang melibatkan sekumpulan pengguna ini. Fungsi manajemen ini dapat dilakukan oleh *Session Initiation Protocol* (SIP). Masalah keamanan merupakan salah satu aspek yang sangat penting pada sebuah sistem informasi. Demikian juga dengan masalah keamanan pada SIP. Meskipun demikian SIP bukanlah protokol yang mudah dijamin keamanannya.

.....

Sumber: *https://openlibrary.telkomuniversity.ac.id/pustaka/files/91178/resume/analisis-aspek-keamanan-voip-pada-next-generation-network-analysis-of-voip-security-aspect-in-next-generation-network-.pdf, diakses 19 Desember 2018, 14.00 WIB*

VoIP memiliki sistem kemanan yang rentan dan dapat dengan mudah dimasuki oleh penyusup. Berdasarkan uraian di atas, buatlah proyek untuk menerapkan *firewall* pada jaringan VoIP. Untuk mempermudah dalam pelaksanaannya, gunakan model pembelajaran *Project Based Learning* dengan melengkapi tahapan-tahapan berikut ini!

A. Perencanaan Kegiatan (Proyek)

Judul Proyek : .....

B. Jenis Tugas : Kelompok

C. Jadwal Pelaksanaan

Tahapan	Tanggal Pelaksanaan	Jenis Kegiatan
1. Persiapan		a. Mencari referensi b. ..... c. ..... d. .....
2. Pelaksanaan		a. ..... b. ..... c. ..... d. .....
3. Pelaporan dan Evaluasi		a. Membuat laporan pembuatan *firewall* b. ..... c. ..... d. .....

D. Sumber Data

1. Pengamatan di lingkungan sekitar
2. Informan (Guru/Teman)
   a. .....
   b. .....
   c. .....
3. Referensi
   a. .....
   b. .....
   c. .....

E. Cara Mengumpulkan Data

1. Observasi
   a. .....
   b. .....
   c. .....
2. Studi *Literature*
   Daftar *Literature*:
   a. .....
   b. .....
   c. .....

F. Analisis Data

1. Hasil Analisis Data Observasi
   a. .....
   b. .....
   c. .....
2. Hasil Analisis Data Studi *Literature*
   a. .....
   b. .....
   c. .....

G. Simpulan Hasil Analisis

.....
.....
.....

Uji Kompetensi

Pilihlah satu jawaban yang paling benar dengan cara memberi tanda silang (X) pada huruf *A, B, C, D,* atau *E* serta tuliskan alasannya!

1. *Firewall* akan mengingat koneksi yang melaluinya sehingga dapat mengizinkan lalu lintas kembali untuk aliran yang sama adalah sifat *firewall* .... .
   A. NGFW
   B. *vulnerability*
   C. *defence*
   D. *deface*
   E. *stateful*

   Alasan: .....
   .....

2. Sebuah program yang menangkap data dari paket yang melewati jaringan seperti *username, password*, dan informasi penting lainnya disebut ....
   A. IP *spoofing*
   B. DoS
   C. *packet snifer*
   D. *hacking*
   E. *malicious code*

   Alasan: .....
   .....

3. Suatu aktivitas menganalisis jaringan untuk mengetahui bagian dari sistem yang cenderung untuk diserang adalah ....
   A. vulnerability
   B. *recommended countermeasures*
   C. *sniffing*
   D. *troubleshooting*
   E. *maintenance*

   Alasan: .....
   .....

4. Proses di mana pengguna harus memberikan *password* yang sudah diatur sebelumnya di dalam sebuah sistem agar pengguna dapat menggunakan suatu jaringan disebut dengan ....
   A. *filtering*
   B. *login*
   C. *recording*
   D. autentifikasi
   E. *user control*

   Alasan: .....
   .....

5. *Firewall* akan memonitor paket yang masuk dan keluar, mengizinkan paket tersebut untuk lewat atau tertahan berdasarkan alamat IP, protokol, dan *port* merupakan cara kerja *firewall* dengan metode ....
   A. inspeksi stateful
   B. *packet filtering*
   C. *behavior control*
   D. *recording*
   E. *screened host firewall*

   Alasan: .....
   .....

6. Serangan keamanan jaringan pada sisi sosial dengan memanfaatkan kepercayaan pengguna disebut ....
   A. *social engineering*
   B. *traffic flooding*
   C. *request flooding*
   D. *spyware*
   E. *deface*

   Alasan: .....
   .....

7. Fungsi *firewall* di dalam jaringan adalah ....
   A. Bertindak sebagai protokol jaringan
   B. Mengganti fungsi dari NAT *gateway*
   C. Menghubungkan jaringan LAN dengan internet
   D. Menerima sinyal dari sebuah komputer yang berada di dalam jaringan
   E. Mengontrol serta mengawasi arus paket data yang mengalir pada jaringan

   Alasan: .....
   .....

8. Seseorang yang tidak memiliki kewenangan tetapi ia mengubah, merusak sumber daya, dan sebagainya. Contohnya mengubah isi pesan atau mengacak program pada sistem, merupakan ancaman yang disebut dengan ....
   A. *pishing*
   B. *denial*
   C. *Interuption*
   D. *modification*
   E. *Interception*

   Alasan: .....
   .....

Perhatikan petunjuk berikut untuk dapat menyelesaikan soal nomor 9 dan 10!

A. Jika pernyataan benar, alasan benar, dan keduanya menunjukkan hubungan sebab akibat.
B. Jika pernyataan benar, alasan benar, tetapi keduanya tidak menunjukkan hubungan sebab akibat.
C. Jika pernyataan benar, alasan salah.
D. Jika pernyataan salah, alasan benar.
E. Jika pernyataan dan alasan salah.

9. *Packet filtering firewall* adalah metode *firewall* di mana paket tersebut tidak akan secara langsung sampai ke *server* tujuan, akan tetapi hanya sampai *firewall* saja.

   Sebab

   Firewall ini akan membuka koneksi baru ke *server* tujuan dan atribut paket, setelahnya paket tersebut akan diperiksa berdasarkan aturan yang berlaku.

Jawaban: .....

Alasan : .....

.....

10. Serangan terhadap keamanan sistem saat ini sering terjadi baik terhadap jaringan komputer ataupun jaringan VoIP. Serangan tersebut bertujuan untuk mencari, mendapatkan, atau mengubah informasi yang terdapat pada sistem. Hal ini dapat dicegah dengan menggunakan *firewall*.

Sebab

Firewall didesain untuk mengizinkan *unprivate* data, menolak layanan yang mudah diserang, serta menjaga jaringan eksternal dari serangan yang dapat menembus *firewall* setiap waktu.

Jawaban: .....

Alasan : .....

.....

Refleksi

Pada Bab V, peserta didik telah mempelajari tentang Menerapkan *Firewall* pada Jaringan VoIP. Materi yang telah dipahami maupun yang belum dipahami akan diberi tanda centang (√) pada kolom di bawah ini. Peserta didik juga akan bertanya jika ada materi yang belum dipahami.

No.	Pernyataan	Keterangan	
		Paham	Belum Paham
1.	Pengertian *firewall*	....	....
2.	.....	....	....
3.	.....	....	....

Muatan Aktivitas Peserta Didik

(Berdasar Permendikbud Nomor 8 Tahun 2016)

A. Tugas Mandiri

1. Jelaskan mengenai pengertian *firewall*!

   .....

   .....

2. Jelaskan bagaimana cara kerja *firewall* pada jaringan komputer!

   .....

   .....

3. Jelaskan cara kerja *firewall* pada jaringan VoIP!

   .....

   .....

4. Jelaskan fungsi *firewall* pada jaringan Komputer!

   .....

   .....

5. Jelaskan fungsi *firewall* pada jaringan VoIP!

   .....

   .....

B. Tugas Kelompok

Setelah mempelajari mengenai penerapan *firewall* pada jaringan VoIP, lakukan aktivitas berikut bersama teman satu kelasmu.

1. Berkelompoklah dengan 3 - 4 temanmu kemudian pilihlah seorang ketua kelompok untuk memimpin diskusi!
2. Bersama anggota kelompokmu, kumpulkan data informasi dari berbagai sumber mengenai perkembangan *firewall* dan penerapannya pada jaringan VoIP yang berada di Indonesia! Tulislah hasil diskusimu secara rinci!

   Hasil diskusi:

   .....

   .....
3. Buatlah suatu kesimpulan mengenai hasil diskusi kelompokmu!

   .....

   .....

C. Tugas Proyek

1. Bentuklah kelompok yang beranggotakan 3-4 orang!
   a. Ketua kelompok : .....
   b. Anggota 1 : .....
   c. Anggota 2 : .....
   d. Anggota 3 : .....
2. Buatlah perencanaan untuk melakukan penerapan *firewall* pada jaringan VoIP yang telah kalian bangun! Perencanaan tersebut meliputi:

   Topologi jaringan VoIP dengan menggunakan *firewall*:

   Konsep jaringan VoIP:

   .....

   .....

   Jenis arsitektur *firewall* yang digunakan:

   .....

   .....

   Konsep *firewall* pada jaringan VoIP:

   .....

   .....
3. Berdasarkan perencanaan yang telah kalian susun, carilah langkah-langkah untuk menerapkan *firewall* pada jaringan VoIP! Tulislah langkah-langkah kerjanya secara rinci!

   Langkah-langkah menerapkan *firewall* pada jaringan VoIP:

   a. .....
   b. .....
   c. .....
   ... .

4. *Screenshoot* setiap proses pengonfigurasian *firewall* tersebut!
5. Setiap kelompok membuat jadwal kegiatan berkaitan dengan perencanaan penerapan *firewall* pada jaringan VoIP seperti pada tabel berikut.

Tabel 5.1 Tabel Tugas Proyek

No.	Tahap	Waktu	Kegiatan
1.	Persiapan	...	...
2.	Pelaksanaan	...	...
3.	Penyusunan hasil kerja	...	...

6. Buatlah laporan tugas proyek penerapan *firewall* pada jaringan VoIP yang telah kalian kerjakan sesuai dengan sistematika penulisan laporan setelah menyelesaikannya dalam waktu dua minggu!

Interaksi Guru dan Orang Tua

Untuk mengisi format tabel interaksi guru dan orang tua, ikuti petunjuk gurumu!

Tabel 5.2 Format Interaksi Guru dan Orang Tua

Nama : ..... NIS. : .....
Kelas : .....

No.	Kompetensi		Keterangan Pencapaian Kompetensi			Paraf Guru	Paraf Orang Tua
			Baik	Cukup	Kurang		
1.	KI 1	Menghayati dan mengamalkan ajaran agama yang dianutnya.	....	....	....	....	....
2.	KI 2	Menghayati dan mengamalkan perilaku jujur, disiplin, santun, peduli (gotong royong, kerja sama, toleran, damai), bertanggung jawab, responsif, dan proaktif melalui keteladanan, pemberian nasihat, penguatan, pembiasaan, dan pengondisian secara berkesinambungan serta menunjukkan sikap sebagai bagian dari solusi atas berbagai permasalahan dalam berinteraksi secara efektif dengan lingkungan sosial dan alam serta dalam menempatkan diri sebagai cerminan bangsa dalam pergaulan dunia.	....	....	....	....	....
3.	KD 3.13	Memahami fungsi *firewall* pada jaringan VoIP.	....	....	....	....	....
4.	KD 4.13	Menalar fungsi *firewall* pada jaringan VoIP.	....	....	....	....	....

Keterangan: Berilah tanda (√) sesuai dengan pencapaian kompetensi peserta didik.