

RENCANA PELAKSANAAN PEMBELAJARAN (RPP) TAHUN PELAJARAN 2021/2022

Sekolah : SMK Binawiyata Karangmalang Sragen
Kelas/Semester : XII TKJ / 5
Mata pelajaran : Administrasi Infrastruktur Jaringan (AIJ)
Materi Pembelajaran : *firewall* jaringan
Alokasi Waktu : 2 Pertemuan (@3 JP x 45 menit = 135 menit)

A. Kompetensi Inti (KI)

1. Menghargai dan menghayati ajaran agama yang dianutnya.
2. Menghargai dan menghayati perilaku jujur, disiplin, tanggung jawab, peduli (toleransi, gotong royong), santun, percaya diri, dalam berinteraksi secara efektif dengan lingkungan sosial dalam jangkauan pergaulan dan keberadaannya.
3. Memahami pengetahuan (faktual, konseptual, dan prosedural) berdasarkan rasa ingin tahunya tentang ilmu pengetahuan, teknologi, seni, budaya terkait fenomena dan kejadian tampak mata.
4. Mencoba, mengolah, dan menyaji dalam ranah konkret (menggunakan, mengurai, merangkai, memodifikasi, dan membuat) dan ranah abstrak (menulis, membaca, menghitung, menggambar, dan mengarang) sesuai dengan yang dipelajari di sekolah dan sumber lain yang sama dalam sudut pandang/teori.

B. Kompetensi Dasar dan Indikator

Kompetensi Dasar	Indikator Pencapaian Kompetensi
1.1 Memahami nilai-nilai keimanan dengan menyadari hubungan keteraturan dan kompleksitas alam dan jagad raya terhadap kebesaran Tuhan yang menciptakannya 1.2 Mendeskripsikan kebesaran Tuhan yang menciptakan berbagai sumber energi di alam 1.3 Mengamalkan nilai-nilai keimanan sesuai dengan ajaran agama dalam kehidupan sehari-hari	1.3.1 Menunjukkan rasa bersyukur dengan berdoa dan memberi salam sebelum dan sesudah menjalankan kegiatan secara konsisten
2.1 Menunjukkan perilaku ilmiah (memiliki rasa ingin tahu, objektif, jujur, teliti, cermat, tekun, hati-hati, bertanggung jawab, terbuka, kritis, kreatif, inovatif dan peduli lingkungan) dalam aktivitas sehari-hari sebagai wujud implementasi sikap dalam melakukan percobaan dan berdiskusi 2.2 Menghargai kerja individu dan kelompok dalam aktivitas sehari-hari sebagai wujud implementasi	2.1.1 Menunjukkan sikap rasa ingin tahu, objektif, jujur, teliti, cermat, tekun, hati-hati, bertanggung jawab, terbuka, kritis, kreatif, inovatif dan peduli lingkungan dalam melaksanakan tugas 2.1.1 Menunjukkan sikap toleransi dalam menerima kesepakatan meskipun berbeda dengan pendapatnya

melaksanakan percobaan dan melaporkan hasil percobaan	
3.10 Mengevaluasi <i>firewall</i> jaringan	3.10.1 Mengidentifikasi tentang <i>firewall</i> jaringan 3.10.2 Menganalisis jenis <i>firewall</i> jaringan 3.10.3 Memilih prosedur dan teknik konfigurasi <i>firewall</i> jaringan (C5)
3.10 Mengkonfigurasi <i>firewall</i> jaringan	4.10.1 Melakukan konfigurasi <i>firewall</i> jaringan (P5) 4.10.2 Menguji hasil konfigurasi <i>firewall</i> jaringan (P5)

C. Tujuan Pembelajaran

1. Peserta didik (A) dapat mengidentifikasi tentang *firewall* jaringan (B) setelah membaca Power point dan melihat literatur *firewall* jaringan (C) dengan tepat dan mandiri (D)
2. Peserta didik (A) mampu menganalisis jenis *firewall* jaringan (B) melalui tayangan video *firewall* jaringan (C) dengan tepat dan mandiri (D)
3. Peserta didik (A) mampu memilih prosedur dan teknik konfigurasi *firewall* jaringan (B) melalui tayangan video *firewall* jaringan (C) dengan percaya diri dan tanggung jawab (D)
4. Peserta didik (A) mampu mengkonfigurasi *firewall* jaringan (B) setelah berdiskusi tentang prosedur dan teknik konfigurasi *firewall* jaringan (C) dengan percaya diri dan tanggung jawab (D)
5. Peserta didik (A) mampu menguji hasil konfigurasi *firewall* jaringan (B) setelah berdiskusi tentang menguji hasil konfigurasi *firewall* jaringan (C) dengan percaya diri dan tanggung jawab (D)

HOTS

HOTS

HOTS

A= Audience; B= Behaviour; C= Condition; D= Degree

D. Materi Pelajaran

1. *Firewall* jaringan
2. Prosedur dan teknik konfigurasi *firewall* jaringan
3. Pengujian Hasil konfigurasi *firewall* jaringan

E. Pendekatan, Model Dan Metode



Pendekatan : Saintifik - TPACK
 Model : (1) Discovery Learning, (2) Project Based Learning
 Metode Pembelajaran : Diskusi, Penugasan, tanya jawab, Eksperimen, presentasi

F. Kegiatan Pembelajaran

Kegiatan	Langkah-langkah Kegiatan Pembelajaran	Nilai Karakter	Kecakapan Abad 21 (4C)	Waktu
Pertemuan 1				
Pendahuluan (Daring Sinkron)	<p>a. Guru mengajak peserta didik bergabung di Google Meet/Zoom (sesi video conference) tepat waktu</p> <p>b. Guru bersama siswa saling memberi dan menjawab salam</p> <p>c. Peserta didik diminta mengisi presensi hadir di Google Form</p> <p>d. Guru menyapa kondisi peserta didik dan mengingatkan tentang aturan protokol kesehatan</p> <p>e. Guru mengajak siswa agar Cinta Tanah Air dan Bangsa</p> <p>f. Guru mengajak peserta didik untuk berdoa, serta memotivasi peserta didik agar belajar dengan giat dan semangat</p> <p>g. Guru bersama peserta didik mereview sekilas materi sebelumnya</p> <p>- Stimulus</p> <p>h. Guru menyampaikan tujuan pembelajaran</p> <p>i. Guru mengajukan pertanyaan yang menantang untuk memotivasi, dan menyampaikan manfaat materi pembelajaran</p> <p>j. Melalui tayangan powerpoint, peserta didik diminta mencermati dan menyimak materi presentasi tentang tujuan dan manfaat, serta jenis <i>firewall</i> jaringan</p> <p>k. Guru memberikan informasi penilaian dan informasi tugas yang mungkin akan dikerjakan</p> <p>l. Sesi video conference ditutup</p>	<p>Disiplin</p> <p>Religius</p> <p>Kemandirian</p> <p>Bertanggung jawab</p> <p>Nasionalis</p> <p>Religius</p> <p>Percaya diri</p>	<p>Communication</p> <p>Collaboration</p> <p>Communication</p> <p>saintifik</p> <p>Communication</p>	20 menit

TPACK

TPACK

Kegiatan	Langkah-langkah Kegiatan Pembelajaran	Nilai Karakter	Kecakapan Abad 21 (4C)	Waktu
Inti (Daring Asinkron)  	<ul style="list-style-type: none"> - Identifikasi Masalah Mengamati <ul style="list-style-type: none"> a. Peserta didik membuka Google Classroom (GCR) mapel TWAN dan mengunduh serta menganalisis sajian materi presentasi tentang tujuan dan manfaat, serta jenis <i>firewall</i> jaringan b. Peserta didik berdiskusi dengan guru melalui WhatsApp group atau GCR dan membuat catatan kecil tentang materi hasil diskusi - Pengumpulan Data Menanya <ul style="list-style-type: none"> c. Peserta didik dimotivasi, merumuskan dan mengajukan pertanyaan-pertanyaan berdasar kan hasil menyimak video materi d. Peserta didik diminta mendiskusikan dan mengidentifikasi cakupan materi tentang tujuan dan manfaat, serta jenis <i>firewall</i> jaringan <i>melalui GCR</i> - Pengolahan Data e. Peserta didik mengunduh file lembar LKPD pertemuan 1 di Google Classroom dan mengumpulkan tepat waktu f. Peserta didik menganalisa soal LKPD dan mengolah data hasil diskusi bersama kelompok siswa dan menuliskannya kedalam LKPD pertemuan 1 - Pembuktian Eksperimen/Eksplorasi g. Peserta didik diminta Mengeksplorasi materi hari ini dengan menyelesaikan latihan soal pengetahuan yang ada di GCR 	Kemandirian Rasa ingin tahu, Kemandirian Kemandirian, tanggungjawab Kemandirian, gotongroyong Kemandirian, tanggungjawab Bekerjasama, saling menghargai pendapat Tanggungjawab, disiplin	saintifik Collaboration HOTS HOTS Saintifik Critical Thinking, HOTS saintifik	95 menit

Kegiatan	Langkah-langkah Kegiatan Pembelajaran	Nilai Karakter	Kecakapan Abad 21 (4C)	Waktu
Penutup (Daring Sinkron)	a. Guru mengajak peserta didik bergabung di Google Meet/Zoom (sesi video conference) tepat waktu - Menarik Kesimpulan Mengkomunikasikan b. Peserta didik menyampaikan hasil diskusi tentang <i>firewall</i> jaringan Asosiasi c. Peserta didik dengan bimbingan guru menyimpulkan tujuan dan manfaat serta jenis <i>firewall</i> jaringan d. Siswa melakukan analisis kelebihan dan kekurangan kegiatan pembelajaran e. Peserta didik diminta untuk mempelajari materi pertemuan berikutnya tentang konfigurasi dan pengujian <i>firewall</i> jaringan f. Pembelajaran diakhiri dengan doa dan salam g. Guru mengakhiri kegiatan belajar dengan menutup sesi video conference	Disiplin Percaya diri, bertanggung jawab Gotong royong Kemandirian Religius	Communication Communication , Collaboration Critical Thinking and Communication	20 menit
Pertemuan 2				
Pendahuluan (Luring)	a. Guru mengajak peserta didik untuk hadir tepat waktu b. Guru bersama siswa saling memberi dan menjawab salam c. Peserta didik diminta mengisi presensi hadir di lembar absensi d. Guru menyapa kondisi peserta didik dan mengingatkan tentang aturan protokol kesehatan e. Guru mengajak siswa agar Cinta Tanah Air dan Bangsa	Disiplin Religius Kemandirian Bertanggung jawab Nasionalis	Communication	20 menit

Kegiatan	Langkah-langkah Kegiatan Pembelajaran	Nilai Karakter	Kecakapan Abad 21 (4C)	Waktu
	f. Guru mengajak peserta didik untuk berdoa , serta memotivasi peserta didik agar belajar dengan giat dan semangat g. Guru bersama peserta didik mereview sekilas materi sebelumnya - Stimulus h. Guru menyampaikan tujuan pembelajaran i. Guru mengajukan pertanyaan yang menantang untuk memotivasi, dan menyampaikan manfaat materi pembelajaran j. Melalui LKPD pertemuan 2 peserta didik diminta mencermati dan menyimak serta melakukan interaksi tanya jawab tentang materi kegiatan konfigurasi dan pengujian <i>firewall</i> jaringan di Google Class room (bisa membuka kembali) k. Guru memberikan informasi penilaian dan informasi tugas yang mungkin akan dikerjakan	Religius Percaya diri	Collaboration Communication Saintifik, Communication	
Inti (Luring)	- Identifikasi Masalah Mengamati a. Peserta didik membuka LKPD pertemuan 2 serta menganalisis sajian materi di LKPD tentang konfigurasi dan pengujian <i>firewall</i> jaringan b. Peserta didik berdiskusi dengan guru dan membuat catatan kecil tentang materi hasil diskusi	Kemandirian, tanggungjawab Kemandirian, gotongroyong	saintifik <i>kolaborasi guru dan siswa</i>	95 menit

TPACK

<p>- Pengumpulan Data Menanya</p> <p>c. Peserta didik dimotivasi, merumuskan dan mengajukan pertanyaan-pertanyaan berdasarkan hasil menyimak LKPD pertemuan 2.</p> <p>d. Peserta didik diminta secara kelompok mendiskusikan dan menyimpulkan cakupan materi tentang konfigurasi dan pengujian <i>firewall</i> jaringan</p> <p>- Pengolahan Data</p> <p>e. Peserta didik menerima lembar LKPD pertemuan 2 dan mengumpulkan tepat waktu</p> <p>f. Peserta didik menganalisa soal kegiatan LKPD pertemuan 2 dan mengolah data hasil diskusi bersama kelompok siswa dan menuliskannya ke dalam LKPD pertemuan 2</p> <p>- Pembuktian Eksperimen/Eksplorasi</p> <p>g. Peserta didik diminta Mengeksplorasi materi hari ini dengan menyelesaikan kegiatan yang ada di LKPD pertemuan 2. Peserta diperbolehkan membuka kembali materi bahan ajar di google classroom</p>	<p>Kemandirian, tanggungjawab</p> <p>Tanggungjawab, disiplin</p> <p>Kemandirian, tanggungjawab, disiplin</p> <p>Tanggungjawab, bekerjasama, menghargai pendapat</p> <p>Kemandirian, tanggungjawab</p>	<p><i>HOTS (C6)</i></p> <p><i>HOTS (C4)</i> saintifik</p> <p>Saintifik</p> <p>Critical Thinking and Communication</p> <p>Saintifik</p>	
---	---	--	--

TPACK

Penutup (Luring)	<p>- Menarik Kesimpulan Mengkomunikasikan</p> <p>a. Peserta didik menyampaikan hasil diskusi tugas LKPD pertemuan 2 tentang konfigurasi dan pengujian <i>firewall</i> jaringan</p> <p>Asosiasi</p> <p>b. Peserta didik dengan bimbingan guru menyimpulkan tentang materi konfigurasi dan pengujian <i>firewall</i> jaringan</p> <p>c. Siswa melakukan analisis kelebihan dan kekurangan kegiatan pembelajaran</p> <p>d. Peserta didik diminta untuk menyiapkan diri mempelajari materi pertemuan berikutnya tentang permasalahan <i>firewall</i> jaringan</p> <p>e. Guru mengakhiri kegiatan belajar dengan doa dan salam</p>	<p>Percaya diri, bertanggung jawab</p> <p>gotongroyong</p> <p>Kemandirian</p> <p>Religius</p>	<p>Communication, scientific</p> <p>Communication, Collaboration</p> <p>Critical Thinking and Communication</p>	<p>20 menit</p>
---------------------	---	---	---	---------------------

G. Media, Alat, dan Sumber Pembelajaran

Media :

1. Materi presentasi tentang *firewall* jaringan
2. Video *firewall* jaringan
3. Video konfigurasi *firewall* jaringan
4. Google Classroom, google drive materi *firewall* jaringan
5. Google Meet/Zoom,
6. Google Form, evaluasi
7. WhatsApp.

Alat :

1. PC di lab computer 1 TKJ sekolah dan Laptop
2. HP Android
3. Hospot/Wifi dan internet di lab computer 1 TKJ sekolah
4. Web Browser

Sumber Belajar :

1. Suryadi Ahmad, 2019, "*Pondok Mikrotik, Kupas tuntas teori, konsep dan praktek seputar dasar-dasar mikrotik*" admisantri56@gmail.com
2. Fajar Adhi Purwaningrum, Eko Agus Darmadi, Agus Purwanto, Vol 2 No 3 (2018): IKRA-ITH INFORMATIKA Vol 2 No 3 Bulan November 2018: jurnal, OPTIMALISASI JARINGAN MENGGUNAKAN FIREWALL, Politeknik Tri Mitra Karya Mandiri , Blok Semper Jomin Baru, Kotabaru, Cikampek – Karawang, link : <https://journals.upi-yai.ac.id/index.php/ikraith-informatika/article/view/251/144>
3. Video Youtube: *firewall* jaringan, link : <https://www.youtube.com/watch?v=fET2PYkckLo>
4. Video Youtube: konfigurasi *firewall* jaringan, link: <https://www.youtube.com/watch?v=5LhE8rN4F3Q>

H. Penilaian

1. Jenis/teknik Penilaian

Penilaian dilakukan selama dan setelah kegiatan pembelajaran, meliputi Penilaian sikap/keaktifan diskusi, pengetahuan maupun ketrampilan melalui penugasan praktik

2. Bentuk instrument

- a. Penilaian Pengetahuan : **Tes tertulis**, Berdasarkan hasil evaluasi di Google Form, dan submission hasil pengamatan video internet gateway
- b. Penilaian Keterampilan : **Hasil Produk**, Berdasarkan hasil presentasi, dan project kelompok
- c. Penilaian Sikap : **Observasi**, Berdasarkan kedisiplinan presensi mengikuti online meeting via Zoom / Google Meet, Kedisiplinan dalam mengumpulkan laporan praktikum dan project, Sikap dan keaktifan bertanya serta menjawab selama sesi online meeting dan diskusi via WhatsApp

3. Program Remedial

Peserta didik yang mendapatkan nilai akhir tiap KD di bawah 70, harus mengikuti program remedial. (dengan mengerjakan ulang).

4. Program Pengayaan

Peserta didik yang mendapatkan nilai 100, mengikuti program pengayaan. Teknik program pengayaan, peserta didik diberi tantangan tugas keterampilan konkret.

Mengetahui,
Kepala SMK Binawiyata

Sragen , Agustus 2021
Guru Mata Pelajaran,

Drs. Saimin, MM, MH

Sujarwoko, ST. SKom

LAMPIRAN

BAHAN AJAR

Sekolah : SMK Binawiyata Karangmalang Sragen
 Kelas/Semester : XII TKJ / 5
 Mata pelajaran : Administrasi Infrastruktur Jaringan (AIJ)
 Materi Pembelajaran : Firewall Jaringan

Kompetensi Dasar dan Indikator

Kompetensi Dasar	Indikator Pencapaian Kompetensi
1.1 Memahami nilai-nilai keimanan dengan menyadari hubungan keteraturan dan kompleksitas alam dan jagad raya terhadap kebesaran Tuhan yang menciptakannya 1.2 Mendeskripsikan kebesaran Tuhan yang menciptakan berbagai sumber energi di alam 1.3 Mengamalkan nilai-nilai keimanan sesuai dengan ajaran agama dalam kehidupan sehari-hari	1.3.1 Menunjukkan rasa bersyukur dengan berdoa dan memberi salam sebelum dan sesudah menjalankan kegiatan secara konsisten
2.1 Menunjukkan perilaku ilmiah (memiliki rasa ingin tahu, objektif, jujur, teliti, cermat, tekun, hati-hati, bertanggung jawab, terbuka, kritis, kreatif, inovatif dan peduli lingkungan) dalam aktivitas sehari-hari sebagai wujud implementasi sikap dalam melakukan percobaan dan berdiskusi 2.2 Menghargai kerja individu dan kelompok dalam aktivitas sehari-hari sebagai wujud implementasi melaksanakan percobaan dan melaporkan hasil percobaan	2.1.1 Menunjukkan sikap rasa ingin tahu, objektif, jujur, teliti, cermat, tekun, hati-hati, bertanggung jawab, terbuka, kritis, kreatif, inovatif dan peduli lingkungan dalam melaksanakan tugas 2.1.1 Menunjukkan sikap toleransi dalam menerima kesepakatan meskipun berbeda dengan pendapatnya
3.10 Mengevaluasi Firewall Jaringan	3.10.1 Mengidentifikasi tentang <i>firewall</i> jaringan 3.10.2 Menganalisis jenis <i>firewall</i> jaringan 3.10.3 Memilih prosedur dan teknik konfigurasi <i>firewall</i> jaringan (C5)
4.10 Mengkonfigurasi Firewall Jaringan	4.10.1 Melakukan konfigurasi <i>firewall</i> jaringan (P5) 4.10.2 Menguji hasil konfigurasi <i>firewall</i> jaringan (P5)

A. Pendahuluan

Keamanan Jaringan adalah proses untuk mencegah dan mengidentifikasi penggunaan yang tidak sah dari jaringan komputer. Langkah-langkah pencegahan membantu menghentikan pengguna yang tidak sah yang disebut “penyusup” untuk mengakses setiap bagian dari sistem jaringan komputer.

Tujuan keamanan jaringan komputer adalah untuk mengantisipasi resiko jaringan komputer berupa bentuk ancaman fisik maupun logic baik langsung ataupun tidak langsung mengganggu aktivitas yang sedang berlangsung dalam jaringan komputer.

Keamanan adalah hal yang penting dalam segala hal. Selayaknya sebuah rumah memiliki pagar, server kita pun membutuhkan 'pagar'. Apalagi server selalu terhubung dengan internet. Isu keamanan sangat penting untuk melindungi server dan data yang tersimpan di dalamnya. 'Pagar' tersebut bernama “firewall” atau “Tembok Api”..

Modul firewall jaringan membahas tentang firewall jaringan dan cara konfigurasinya yang tujuan akhirnya memiliki bekal awal bagi peserta didik untuk mempelajari modul selanjutnya dalam Keahlian TKI ini.

Setelah mempelajari modul ini peserta didik dapat: menganalisis dan mengkonfigurasi internet gateway (NAT).

Proses pembelajaran untuk materi ini dapat berjalan dengan baik apabila mengikuti langkah-langkah belajar sebagai berikut:

- Pahami dulu kegiatan penting dalam program pelatihan ini dengan memperhatikan isi capaian pembelajaran setiap kegiatan belajar
- Lakukan kajian terhadap setiap sub materi, agar memudahkan proses pembelajaran.
- Pelajari dahulu materi, dan diakhir kegiatan belajar dapat menyelesaikan tugas yang harus dikerjakan secara langsung
- Keberhasilan program pembelajaran ini tergantung dengan kesungguhan dalam mengerjakan setiap tugas dalam kegiatan belajar ini
- Bila menemukan kesulitan, silahkan hubungi instruktur pembimbing

1. *Diskripsi singkat*

Modul bahan ajar ini menjelaskan tentang firewall jaringan dan firewall jaringan. Di dalam pembahasannya diuraikan tentang konsep dan jenis firewall jaringan, serta cara konfigurasi dan pengujiannya.

2. *Relevansi*

Kegiatan belajar modul ini memiliki relevansi dengan materi pada modul-modul selanjutnya (Administrasi Infrastruktur Jaringan). Penyajian materi yang sistematis dan teratur membawa keterbacaan modul ini menarik karena disertai dengan gambar, contoh-contoh aplikatif dengan tuntutan dunia kerja di industri dan masyarakat. Karakteristik modul ini menawarkan metode PjBL (Project Based Learning). Hal ini untuk mendorong peserta didik agar dapat :

- Memahami , menguasai dan menganalisis firewall jaringan
- Meningkatkan rasa ingin tahu manfaat-manfaat firewall jaringan
- Meningkatkan pemahaman dan keterampilan mengenai firewall jaringan dengan sikap yang baik.
- Menganalisis jenis-jenis, efisiensi dan masalah yang berkaitan dengan firewall jaringan.
- Mengkonfigurasi dan uji koneksi firewall jaringan.

3. *Petunjuk belajar*

Dalam mempelajari modul ini, sebagai prasyarat peserta didik telah mampu membuat gateway internet yang telah dipelajari pada pertemuan sebelumnya.

Untuk membantu para peserta didik dalam menguasai firewall jaringan yaitu

dengan mempelajari secara berurutan bagian demi bagian dalam materi bahan ajar ini, karena masing-masing saling berkaitan. Dalam kegiatan belajar ini dilengkapi dengan uji uji kompetensi yang menjadi alat ukur tingkat penguasaan setelah mempelajari materi dalam modul ini. Jika belum menguasai 70 % dari setiap kegiatan, maka dapat mengulangi untuk mempelajari materi yang tersedia dalam modul ini. Apabila Anda masih mengalami kesulitan memahami materi yang ada dalam modul ini, silahkan diskusikan dengan teman atau instruktur.

B. Inti

1. *Capaian pembelajaran*

Setelah mengikuti seluruh tahapan pada kegiatan belajar ini, peserta didik akan mampu menguasai konseptual dan cara konfigurasi firewall jaringan

2. *Sub Capaian pembelajaran*

2.1. Peserta didik (A) dapat **mengidentifikasi** tentang *firewall* jaringan (B) setelah membaca Power point dan melihat literatur *firewall* jaringan (C) dengan tepat dan mandiri (D)

2.2. Peserta didik (A) mampu **menganalisis** jenis *firewall* jaringan (B) melalui tayangan video *firewall* jaringan (C) dengan tepat dan mandiri (D)

2.3. Peserta didik (A) mampu **memilih** prosedur dan teknik konfigurasi *firewall* jaringan (B) melalui tayangan video *firewall* jaringan (C) dengan percaya diri dan tanggung jawab (D)

2.4. Peserta didik (A) mampu **mengkonfigurasi** *firewall* jaringan (B) setelah berdiskusi tentang prosedur dan teknik konfigurasi *firewall* jaringan (C) dengan percaya diri dan tanggung jawab (D)

2.5. Peserta didik (A) mampu **menguji** hasil konfigurasi *firewall* jaringan (B) setelah berdiskusi tentang menguji hasil konfigurasi *firewall* jaringan (C) dengan percaya diri dan tanggung jawab (D)

A= Audience; B= Behaviour; C= Condition; D= Degree

HOTS

HOTS

HOTS

3. Uraian Materi

1. Firewall Jaringan

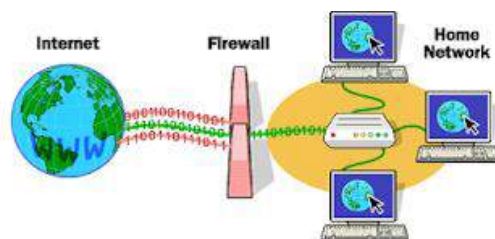
Studi Kasus Firewall Jaringan

Tujuan keamanan jaringan komputer adalah untuk mengantisipasi resiko jaringan komputer berupa bentuk ancaman fisik maupun logic baik langsung ataupun tidak langsung mengganggu aktivitas yang sedang berlangsung dalam jaringan komputer.

Di Lab 2 TKJ SMK Binawiyata ini, setiap siswa secara bebas bisa mengakses youtube melalui hp androidnya tanpa ada pembatasan. Hal ini akan sangat mengganggu konsentrasi siswa di saat pembelajaran desain. Untuk itu diperlukan pembatasan akses, agar siswa dapat focus dengan pembelajaran yang sedang berlangsung. Pembatasan tersebut adalah, melalui port yang tersambung ke AP (Hospot) pada mikrotik, akan diberikan pengaturan keamanan agar melalui port tersebut, siswa tidak bisa mengakses youtube.

Untuk mendukung kebutuhan pembatasan akses (keamanan jaringan) yang ada di lab 2 TKJ SMK Binawiyata tersebut maka diperlukan sebuah firewall jaringan yang dikonfigurasi sesuai dengan kebutuhan (pembatasan akses youtube) melalui port Hossport di mikrotik.

Pengertian Firewall Jaringan



Gambar 1.1 Arsitektur Firewall Dalam Jaringan

Istilah “firewall” sendiri sebenarnya juga dikenal dalam disiplin lain, dan dalam kenyataannya, istilah ini tidak hanya bersangkutan dengan terminology jaringan. Kita juga menggunakan firewall, misalnya untuk memisahkan garasi dari rumah, atau memisahkan satu apartemen dengan apartemen lainnya. Dalam hal ini, firewall adalah penahan (barrier) terhadap api yang dimaksudkan untuk memperlambat penyebaran api seandainya terjadi kebakaran sebelum petugas pemadam kebakaran datang untuk memadamkan api. Contoh lain dari firewall juga bisa ditemui pada kendaraan bermotor, dimana firewall memisahkan antara ruang penumpang dan kompartemen mesin.

Untuk firewall didalam terminology jaringan, memiliki beberapa pengertian antara lain adalah sebagai berikut:

- Firewall didefinisikan sebagai suatu cara atau mekanisme yang diterapkan baik terhadap hardware, software ataupun system itu sendiri dengan tujuan untuk melindungi, baik dengan menyaring, membatasi atau bahkan menolak suatu atau semua hubungan/kegiatan suatu segmen pada jaringan pribadi dengan jaringan luar yang bukan merupakan ruang lingkungannya.
- Firewall didefinisikan sebagai sebuah komponen atau kumpulan komponen yang membatasi akses antara sebuah jaringan yang diproteksi dan internet, atau antara kumpulan kumpulan jaringan lainnya.
- Definisi lain mengatakan bahwa, firewall adalah sebuah computer yang memproteksi jaringan dari jaringan yang tidak dipercaya yang memisahkan antara jaringan local dengan jaringan publik, dengan melakukan metode filtering paket data yang masuk dan keluar.
- Menurut Wabopedia.com definisi firewall adalah sebuah sistem yang didesain untuk

mencegah akses yang tidak sah ke atau dari jaringan pribadi (Privat Network). Sedangkan menurut MTCNA definisinya adalah firewall diposisikan antara jaringan lokal dan jaringan publik bertujuan melindungi computer dari serangan, dan secara efektif mengontrol koneksi data menuju, dari dan melewati router.

- Ilmuwan lain mendefinisikan firewall sebagai sebuah titik diantara dua/lebih jaringan dimana semua lalu lintas (trafik) harus melaluinya (choke point); trafik dapat dikendalikan oleh dan diautentifikasi melalui suatu perangkat, dan seluruh trafik selalu dalam kondisi tercatat (logged).

Dari beberapa definisi diatas, penulis dapat memberikan definisi dimana firewall adalah sebuah pembatas antara suatu jaringan local dengan jaringan lainnya yang sifatnya public (dapat diakses oleh siapapun) sehingga setiap data yang masuk dapat diidentifikasi untuk dilakukan penyaringan sehingga aliran data dapat dikendalikan untuk mencegah bahaya/ancaman yang datang dari jaringan publik.

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 berkaitan dengan hardware (pengamanan fisik, sumber daya listrik) maupun yang berkaitan dengan software (sistem, konfigurasi, sistem akses, dll). Gangguan pada sistem dapat terjadi karena faktor ketidaksengajaan yang dilakukan oleh pengelola (human error), akan tetapi tidak sedikit pula yang disebabkan oleh pihak ketiga. Gangguan dapat berupa kerusakan, penyusutan, pencurian hak akses, penyalahgunaan data maupun sistem, sampai tindakan kriminal melalui aplikasi jaringan komputer. Pengamanan terhadap sistem hendaknya dilakukan sebelum sistem tersebut difungsikan. Percobaan koneksi (trial) sebaiknya dilakukan sebelum sistem yang sebenarnya difungsikan. Dalam melakukan persiapan fungsi sistem hendaknya disiapkan pengamanan dalam bentuk:

- Memisahkan terminal yang difungsikan sebagai pengendali jaringan atau titik pusat akses (Server) pada suatu area yang digunakan untuk aplikasi tertentu.
- Menyediakan pengamanan fisik berupa ruangan khusus untuk pengamanan perangkat yang disebut pada butir nomor 1. Ruangan tersebut dapat diberikan label Network Operating Center (NOC) dengan membatasi personil yang diperbolehkan masuk.
- Memisahkan sumber daya listrik untuk NOC dari pemakaian yang lain. Hal ini untuk menjaga kestabilan fungsi sistem. Perlu juga difungsikan Uninterruptable Power Supply (UPS) dan Stabilizer untuk menjaga kestabilan supply listrik yang diperlukan perangkat pada NOC.
- Merapikan wiring ruangan dan memberikan label serta pengklasifikasian kabel.
- Memberikan Soft Security berupa Sistem Firewall pada perangkat yang difungsikan di jaringan.
- Merencanakan maintenance dan menyiapkan Back Up sistem.

Firewall adalah salah satu aplikasi pada sistem operasi yang dibutuhkan oleh jaringan komputer untuk melindungi integritas data/sistem jaringan dari serang-serangan pihak yang tidak bertanggung jawab atau lalu lintas jaringan yang tidak aman. Caranya dengan melakukan filterisasi terhadap paket-paket yang melewatinya.

Firewall tersusun dari aturan-aturan yang diterapkan baik terhadap hardware, software ataupun sistem itu sendiri dengan tujuan untuk melindungi jaringan, baik dengan melakukan filterisasi, membatasi, ataupun menolak suatu permintaan koneksi dari jaringan luar lainnya seperti internet.

Oleh karena seringnya firewall digunakan untuk melindungi jaringannya, maka firewall juga berfungsi sebagai pintu penyangga antara jaringan yang dilindunginya dengan jaringan lainnya atau biasa disebut gateway.

Pada firewall terjadi beberapa proses yang memungkinkannya melindungi jaringan. Proses yang terjadi pada firewall ada tiga macam yaitu:

1. Modifikasi header paket,
2. Translasi alamat jaringan, dan
3. Filter paket

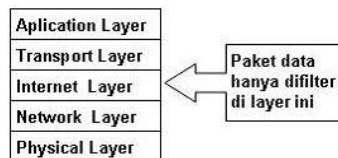
Modifikasi header paket digunakan untuk memodifikasi kualitas layanan bit paket TCP sebelum mengalami proses routing.

Translasi alamat jaringan antara jaringan privat dan jaringan publik terjadi pada firewall. Translasi yang terjadi dapat berupa translasi satu ke satu (one to one), yaitu satu alamat IP privat dipetakan kesatu alamat IP publik atau translasi banyak kesatu (many to one) yaitu beberapa alamat IP privat dipetakan kesatu alamat publik.

Filter paket digunakan untuk menentukan nasib paket apakah dapat diteruskan atau tidak.

2. Jenis-jenis Firewall

a. Packet Filtering Gateway



Gambar 2.1 Lapisan Untuk Proses Packet Filtering Gateway

Packet filtering gateway dapat diartikan sebagai firewall yang bertugas melakukan filterisasi terhadap paket-paket yang datang dari luar jaringan yang dilindunginya.

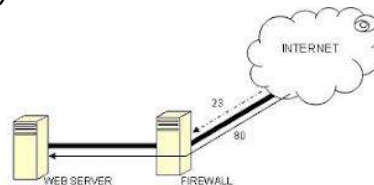
Filterisasi paket ini hanya terbatas pada sumber paket, tujuan paket, dan atribut-atribut dari paket tersebut, misalnya paket tersebut bertujuan ke server kita yang menggunakan alamat IP 202.51.226.35 dengan port 80. Port 80 adalah atribut yang dimiliki oleh paket tersebut.

Seperti yang terlihat pada gambar, firewall tersebut akan melewatkan paket dengan tujuan ke Web Server yang menggunakan port 80 dan menolak paket yang menuju Web Server dengan port 23.

Bila kita lihat dari sisi arsitektur TCP/IP, firewall ini akan bekerja pada layer internet. Firewall ini biasanya merupakan bagian dari sebuah router firewall.

Software yang dapat digunakan untuk implementasi packet filtering diantaranya adalah iptables dan ipforward.

b. Application Layer Gateway

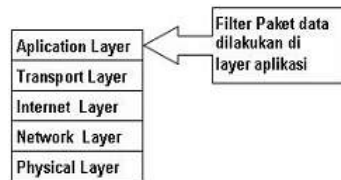


Gambar 2.2 Web Server Dengan Firewall

Mekanisme lainnya yang terjadi adalah paket tersebut tidak akan secara langsung sampai ke server tujuan, akan tetapi hanya sampai firewall saja.

Selebihnya firewall ini akan membuka koneksi baru ke server tujuan setelah paket tersebut diperiksa berdasarkan aturan yang berlaku.

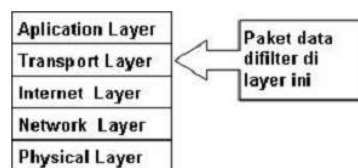
Bila kita melihat dari sisi layer TCP/IP, firewall jenis ini akan melakukan filterisasi pada layer aplikasi (Application Layer).



Gambar 2.3 Proxy Firewall Dilihat Pada Model TCP/IP

c. *Circuit Level Gateway*

Model firewall ini bekerja pada bagian Lapisan Transport model referensi TCP/IP. Firewall ini akan melakukan pengawasan terhadap awal hubungan TCP yang biasa disebut sebagai TCP Handshaking, yaitu proses untuk menentukan apakah sesi hubungan tersebut diperbolehkan atau tidak. Bentuknya hampir sama dengan Application Layer Gateway, hanya saja bagian yang difilter terdapat ada lapisan yang berbeda, yaitu berada pada layer Transport.

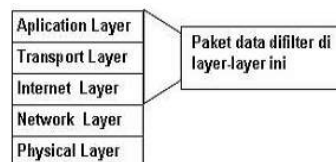


Gambar 2.4 Circuit Level Gateway Dilihat Pada Model TCP/IP

d. *Statefull Multilayer Inspection Firewall*

Model firewall ini merupakan penggabungan dari ketiga firewall sebelumnya. Firewall jenis ini akan bekerja pada lapisan Aplikasi, Transport dan Internet.

Dengan penggabungan ketiga model firewall yaitu Packet Filtering Gateway, Application Layer Gateway dan Circuit Level Gateway, mungkin dapat dikatakan firewall jenis ini merupakan firewall yang memberikan fitur terbanyak dan memberikan tingkat keamanan yang paling tinggi.



Gambar 2.5 State Multilayer Inspection Firewall Dilihat Pada Model TCP/IP

3. Fitur Mikrotik Firewall

Didalam router mikrotik juga terdapat fitur firewall yang berfungsi untuk melindungi dengan cara mendrop atau mengaccept sebuah paket yang akan masuk, melewati, atau keluar router.

Dalam fitur firewall terdapat beberapa direktori yaitu :

1. Rules
2. Nat (source-nat and destination-nat)
3. Mangle
4. Address List
5. Layer 7 Protocol (baru di versi 3)
6. Service Ports
7. Connections

Sistem monitor yang ada di firewall:

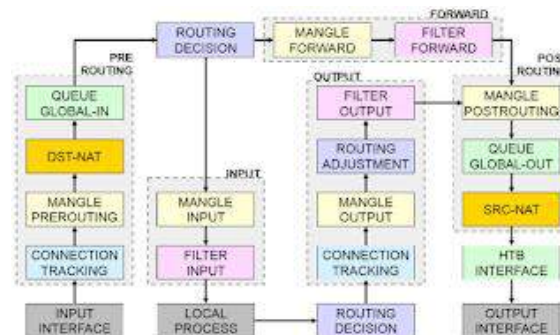
Traffic Flow

Traffic-Flow merupakan sebuah sistem yang menampilkan informasi statistik akan besar atau banyaknya paket-paket yang melewati sebuah router. Maka dengan fitur ini kita bisa melakukan monitoring terhadap sebuah jaringan dan memungkinkan bagi kita untuk mengidentifikasi berbagai macam masalah yang terjadi di dalamnya. Selain itu, dengan memanfaatkan fitur ini kita dapat melakukan analisa dan meningkatkan performa dari router.

Setiap paket data memiliki asal (source) dan tujuan (destination). Traffic flow bisa dibedakan menjadi 3 kategori, dilihat dari sudut pandang router.

- Dari Luar router menuju ke luar router lagi.
Contoh : traffic client browsing ke internet
- Dari luar router menuju ke dalam router itu sendiri (Local process).
Contoh : traffic winbox ke router
- Dari dalam router (local process) menuju ke luar router.
Contoh : traffic ping dari new terminal winbox

Simple Packet Flow



Gambar 2.6 Simple Packet Flow

Di dalam packet flow terdapat 5 pos pemeriksaan didalamnya yaitu:

1. Input: pos pemeriksaan paket data yang terletak di depan Local Proses, semua data yang menuju ke dalam router itu sendiri (Local Proses) akan melewati pos ini.
2. Output: pos pemeriksaan paket data yang terletak di belakang Local Proses, semua paket data yang keluar dari dalam router (local proses) sebelum menuju ke output interface akan di proses dalam chain output.
3. Forward: pos pemeriksaan paket data yang terletak di antara PreRouting dan PostRouting ,semua paket data dari luar router menuju ke luar router akan diproses di chain Forward.
4. Prerouting: pos pemeriksaan paket data yang terletak dibelakang input interface,semua data yang masuk dari input interface akan melalui dan diproses pada chain Prerouting sebelum ke proses selanjutnya.
5. Postrouting: Postrouting = pos pemeriksaan yang terletak di depan output interface,semua data yang keluar menuju output interface akan terlebih dahulu di proses pada Chain Post Routing.

Connection Tracking and State

- Connection Tracking

Connection Tracking adalah “jantung” dari firewall, mengumpulkan informasi tentang active connections. Dengan mendisable connection tracking router akan kehilangan fungsi NAT, filter rule dan mangle. Setiap connection tracking membaca pertukaran traffic 2 arah (src dan dst address). Connection tracking membutuhkan

- CPU resources (disable saja jika kita tidak menggunakan firewall).
- Connection tracking mempunyai kemampuan untuk melihat informasi koneksi yang melewati router, seperti source dan destination IP dan Port yang sedang di gunakan, status koneksi, tipe protocol dan lain-lain.

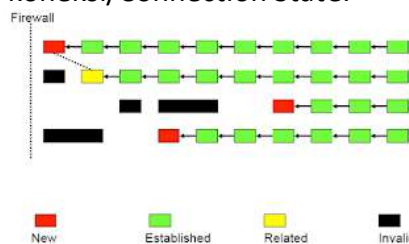
	Src. Address	Dest. Address	Proto	Connests	Connests.	P2P	Timeout	TCP State
U	192.168.1.12	239.192.1.1	2 (p)				00:10:30	
A	192.168.1.12	202.73.36.32:123	17 (u)				00:02:35	
U	192.168.1.254	224.0.0.1	2 (p)				00:10:20	
A	192.168.88.2:51964	173.202.113.17:443	6 (tcp)				1d 00:00	established
A	192.168.88.2:51979	173.202.173.52:443	6 (tcp)				1d 00:00	established
A	192.168.88.2:51980	31.13.75.33:443	6 (tcp)				1d 00:00	established
A	192.168.88.2:51981	23.58.43.27:80	6 (tcp)				1d 00:00	established
A	192.168.88.2:51982	23.58.43.27:80	6 (tcp)				1d 00:00	established
A	192.168.88.2:51984	23.62.109.152:443	6 (tcp)				1d 00:00	established
U	192.168.88.2:52257	255.255.255.255:20	17 (u)				00:00:43	
A	192.168.88.2:64100	8.8.8.8:53	17 (u)				00:03:11	

Gambar 2.7 Connection tracking

Setiap paket data itu memiliki status koneksi (connection started) yang dapat dilihat pada connection tracking, ini gan, status koneksi nya :

- ✓ Invalid : paket tidak dimiliki oleh koneksi apapun, tidak berguna.
- ✓ New : paket yang merupakan pembuka sebuah koneksi/paket pertama dari sebuah koneksi.
- ✓ Established : merupakan paket kelanjutan dari paket dengan status new.
- ✓ Related : paket pembuka sebuah koneksi baru, tetapi masih berhubungan dengan koneksi sebelumnya.

Berikut gambaran Status koneksi/Connection State.



Gambar 2.8 Status koneksi/Connection State

Implikasi Connection State

Pada rule Firewall filter, pada baris paling atas biasanya kita membuat rule :

1. Connection state=invalid >> drop
2. Connection state=related >> accept
3. Connection state=established >> accept
4. Connection state=new >> diproses ke rule berikutnya

Sistem rule seperti ini akan sangat menghemat resources router, karena proses filtering hanya dilakukan pada saat connection dimulai (connection-state=new).

Mangle

Mangle adalah cara untuk menandai paket-paket data tertentu, dan kita akan menggunakan tanda tersebut pada fitur lainnya, misalnya pada filter, routing, NAT, ataupun queue. Pada mangle kita juga bisa melakukan perubahan beberapa parameter pada IP Header, misalnya TOS (DSCP) dan TTL fields. Tanda mangle ini hanya bisa digunakan pada router yang sama, dan tidak terbaca pada router lainnya. Pembacaan rule mangle akan dilakukan dari atas ke bawah secara berurutan.

	→	→	→
Prerouting	yes	yes	no
Input	yes	no	no
Forward	no	yes	no
Output	no	no	yes
Postrouting	no	yes	yes

Gambar2.9 Chain pada Mangle

Type Of Mark

Ada tiga tipe mark, diantaranya ialah :

1. **Packet Mark:** Penandaan untuk setiap paket data
2. **Connection Mark:** Penandaan untuk koneksi
3. **Route Mark:** Penandaan paket khusus untuk routing

Pada saat yang bersamaan, setiap paket data hanya bisa memiliki 1 conn-mark, 1 packet-mark, dan 1 route-mark.

Connection Mark Adalah fitur mangle untuk menandai suatu koneksi (berlaku baik untuk request, maupun untuk response) sebagai satu kesatuan. Untuk jaringan dengan src-nat atau kalau kita mau melakukan marking berdasarkan protokol tcp, disarankan untuk melakukan mark-connection terlebih dahulu, baru membuat mark-packet atau mark-routing berdasarkan conn-mark nya. Mark-connection cukup dibuat pada saat proses request saja.

Passthrough

Passthrough=no

- berarti jika parameter sesuai, maka baris mangle berikutnya tidak lagi dibaca
- value mangle sudah final, tidak diubah lagi

Passthrough=yes

- akan tetap membaca baris mangle berikutnya
- value mangle bisa diubah lagi di baris berikutnya

Biasanya pada :

- mark-connection, passthrough = yes
- mark-packet, passthrough=no

Mangle dengan SRC NAT




Karena urutan proses NAT dan mangle diperhatikan pada bagan **Packet Flow**, maka kita harus menggunakan conn-mark terlebih dahulu jika kita ingin membuat mangle untuk menandai proses uplink dan downlink IP tertentu di chain **Prerouting**. Jika dipasang mangle di chain **Forward** maka bisa langsung digunakan packet mark.

Chain pada Firewall Mikrotik

Firewall beroperasi dengan menggunakan aturan firewall. Setiap aturan terdiri dari dua bagian - matcher yang sesuai arus lalu lintas terhadap kondisi yang diberikan dan tindakan yang mendefinisikan apa yang harus dilakukan dengan paket yang cocok. Aturan firewall filtering dikelompokkan bersama dalam chain. Hal ini memungkinkan paket yang akan dicocokkan terhadap satu kriteria umum dalam satu chain, dan kemudian melewati untuk pengolahan terhadap beberapa kriteria umum lainnya untuk chain yang lain.

Misalnya paket harus cocok dengan alamat IP:port. Tentu saja, itu bisa dicapai dengan menambahkan beberapa rules dengan alamat IP:port yang sesuai menggunakan

chain forward, tetapi cara yang lebih baik bisa menambahkan satu rule yang cocok dengan lalu lintas dari alamat IP tertentu, misalnya: filter firewall / ip add src-address = 1.1.1.2/32 jump-target = "mychain".

			
Prerouting	not implemented	not implemented	not implemented
Input	yes	no	no
Forward	no	yes	no
Output	no	no	yes
Postrouting	not implemented	not implemented	not implemented

Gambar2.10 Chain pada firewall mikrotik

Ada tiga chain yang telah ditetapkan pada RouterOS Mikrotik :

1. Input - digunakan untuk memproses paket memasuki router melalui salah satu interface dengan alamat IP tujuan yang merupakan salah satu alamat router. Chain input berguna untuk membatasi akses konfigurasi terhadap Router Mikrotik.
2. Forward - digunakan untuk proses paket data yang melewati router.
3. Output - digunakan untuk proses paket data yang berasal dari router dan meninggalkan melalui salah satu interface.

Posisi Chain / Parent

From	To	Mangle	Firewall	Queue
Outside	Router/ Local Process	Prerouting		Global-In
		Input	Input	Global-Total
Router/ Local Process	Outside	Output	Output	Global-Out
		Postrouting		Global-Total
Outside	Outside	Prerouting		Interface
		Forward	Forward	Global-In
		Postrouting		Global-Out
				Global-Total
				Interface

Gambar2.11 Posisi Chain/Parent

Ketika memproses chain, rule yang diambil dari chain dalam daftar urutan akan dieksekusi dari atas ke bawah. Jika paket cocok dengan kriteria aturan tersebut, maka tindakan tertentu dilakukan di atasnya, dan tidak ada lagi aturan yang diproses dalam chain. Jika paket tidak cocok dengan salah satu rule dalam chain, maka paket itu akan diterima.

Firewall Filters – Blocking Rules

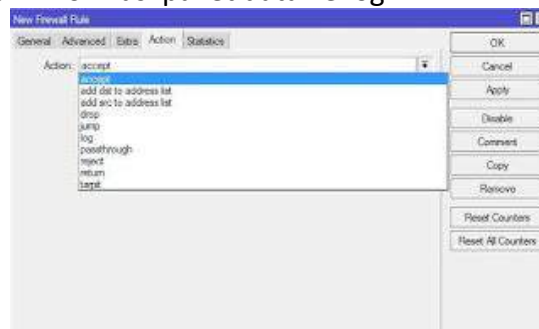
- Adalah cara untuk memfilter paket, dilakukan untuk meningkatkan keamanan jaringan, dan mengatur flow data dari, ke client, ataupun router
- Pembacaan rule filter dilakukan dari atas ke bawah secara berurutan. Jika melewati rule yang kriterianya sesuai akan dilakukan action yang ditentukan, jika tidak sesuai, akan dianalisa ke baris selanjutnya.

Action Filter Firewall RouterOS Mikrotik

Pada konfigurasi firewall mikrotik ada beberapa pilihan Action, diantaranya :

- Accept : paket diterima dan tidak melanjutkan membaca baris berikutnya
- Drop : menolak paket secara diam-diam (tidak mengirimkan pesan penolakan ICMP)
- Reject : menolak paket dan mengirimkan pesan penolakan ICMP
- Jump : melompat ke chain lain yang ditentukan oleh nilai parameter jump-target
- Tarptit : menolak, tetapi tetap menjaga TCP connection yang masuk (membalas dengan SYN/ACK untuk paket TCP SYN yang masuk)

- Passthrough : mengabaikan rule ini dan menuju ke rule selanjutnya
- log : menambahkan informasi paket data ke log

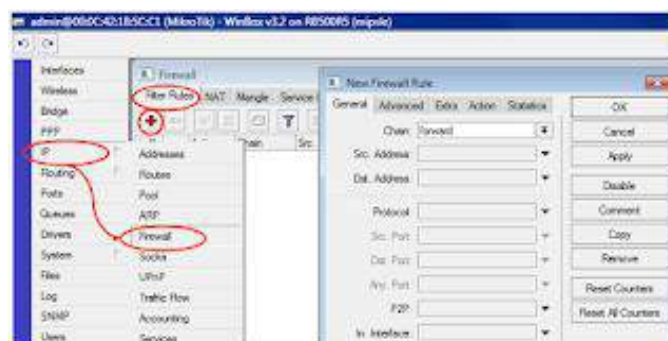


Gambar2.12 Action Filter Firewall RouterOS Mikrotik

Filter Rules

Filter rule biasanya digunakan untuk melakukan kebijakan boleh atau tidaknya sebuah trafik ada dalam jaringan, identik dengan accept atau drop. Pada menu **Firewall** → **Filter Rules** terdapat 3 macam chain yang tersedia. Chain tersebut antara lain adalah **Forward**, **Input**, **Output**. Adapun fungsi dari masing-masing chain tersebut adalah sebagai berikut:

- **Forward** : Digunakan untuk memproses trafik paket data yang hanya melewati router. Misalnya trafik dari jaringan public ke local atau sebaliknya dari jaringan local ke public, contoh kasus seperti pada saat kita melakukan browsing. Trafik laptop browsing ke internet dapat dimanage oleh firewall dengan menggunakan chain forward.
- **Input** : Digunakan untuk memproses trafik paket data yang masuk ke dalam router melalui interface yang ada di router dan memiliki tujuan IP Address berupa ip yang terdapat pada router. Jenis trafik ini bisa berasal dari jaringan public maupun dari jaringan lokal dengan tujuan router itu sendiri. Contoh: Mengakses router menggunakan winbox, webfig, telnet baik dari Public maupun Local.
- **Output** : Digunakan untuk memproses trafik paket data yang keluar dari router. Dengan kata lain merupakan kebalikan dari 'Input'. Jadi trafik yang berasal dari dalam router itu sendiri dengan tujuan jaringan Public maupun jaringan Local. Misal dari new terminal winbox, kita ping ke ip google. Maka trafik ini bisa ditangkap dichain output.



Gambar2.13 Filter Rule

Basis Address List

Address-list digunakan untuk memfilter group IP address dengan 1 rule firewall. Address-list juga bisa merupakan list IP hasil dari rule firewall yang memiliki action "add to address list". Satu line address-list dapat berupa subnet, range, atau 1 host IP address.

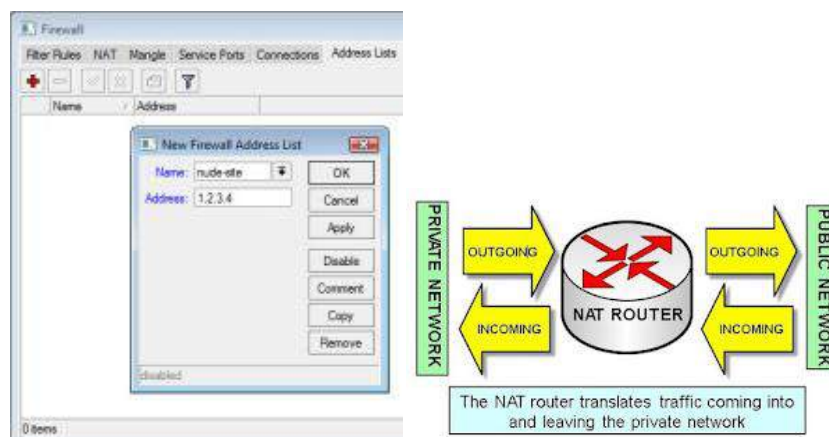
Kita dapat melakukan pengelompokan IP Address dengan Address List. Address List (seperti halnya mangle) bisa dijadikan parameter dalam pembuatan filter, queue, mangle, NAT, dll. Dengan Filter dan Mangle, kita bisa secara otomatis memasukkan IP Address tertentu ke dalam address list dan juga menentukan jangka waktu expire nya.

NAT (Network Address Translation)

NAT (Network Address Translation) atau Penafsiran alamat jaringan adalah suatu metode untuk menghubungkan lebih dari satu komputer ke jaringan internet dengan menggunakan satu alamat IP. Banyaknya penggunaan metode ini disebabkan karena ketersediaan alamat IP yang terbatas, kebutuhan akan keamanan (security), dan kemudahan serta fleksibilitas dalam administrasi jaringan.

NAT merupakan salah satu protocol dalam suatu sistem jaringan, NAT memungkinkan suatu jaringan dengan ip atau internet protocol yang bersifat privat atau privat ip yang sifatnya belum teregistrasi di jaringan internet untuk mengakses jalur internet, hal ini berarti suatu alamat ip dapat mengakses internet dengan menggunakan ip privat atau bukan menggunakan ip public, NAT biasanya dibenamkan dalam sebuah router, NAT juga sering digunakan untuk menggabungkan atau menghubungkan dua jaringan yang berbeda, dan mentranslate atau menterjemahkan ip privat atau bukan ip public dalam jaringan internal ke dalam jaringan yang legal network sehingga memiliki hak untuk melakukan akses data dalam sebuah jaringan.

NAT digunakan untuk melakukan perubahan baik src-address ataupun dst-address. Setelah paket data pertama dari sebuah koneksi terkena NAT, maka paket berikutnya pada koneksi tersebut juga akan terkena NAT. NAT akan diproses terurut mulai baris paling atas hingga ke bawah.



Gambar2.14 Firewall NAT Pada Winbox

Di MikroTik ada dua type NAT :

- ✓ Srcnat (Source NAT) : pengalihan dijalankan untuk paket data yang berasal dari jaringan natted. NAT dapat merubah alamat IP asal paket dari jaringan natted dengan alamat IP umum. Source NAT senantiasa dikerjakan sesudah routing saat sebelum paket keluar menuju jaringan. Masquerade yaitu perumpamaan dari srcnat.
- ✓ Dstnat (Destination NAT) : pengalihan dikerjakan untuk paket data yang menuju

jaringan lokal. Ini umum difungsikan untuk membuat host dalam jaringan lokal dapat diakses dari luar jaringan (internet). NAT dapat merubah alamat IP arah paket dengan alamat IP lokal. Destination NAT senantiasa dikerjakan saat sebelum routing saat paket dapat masuk dari jaringan. Port Forward, Port Mapping, transparent proxy yaitu perumpamaan dari dstnat.

Src-NAT and Masquerade

Untuk menyembunyikan IP Address lokal dan menggantikannya dengan IP Address publik yang sudah terpasang pada router

src-nat: Kita bisa memilih IP Address publik yang digunakan untuk menggantikan.

Masquerade: Masquerade mungkin bisa di artikan sebagai topeng untuk bisa terkoneksi ke jaringan internet menggunakan ip private, atau simplenya masquerade mikrotik atau masquerade linux merupakan sebuah metode yang mengizinkan dan memperbolehkan ip private untuk terkoneksi ke internet dengan menggunakan bantuan sebuah ip public /bertopengkan sebuah ip publik.

Dengan bantuan masquerade sebuah ip publik dapat mendistribusikan koneksi internet ke banyak ip private. Ip private merupakan ip address yang tidak masuk kedalam routing table router jaringan internet global. Dan ip private hanya bisa di gunakan didalam jaringan lokal. Karena ip private ini hanya bisa di gunakan dalam jaringan LAN atau local area network, maka lahirlah masquerade yang menjadi topeng agar ip private (LAN) dapat berinteraksi ke internet.

Secara otomatis akan menggunakan IP Address pada interface publik. Digunakan untuk mempermudah instalasi dan bila IP Address publik pada interface public menggunakan IP Address yang dinamik (misalnya DHCP, PPTP atau EoIP)

Dst-nat and Redirect

Untuk melakukan penggantian IP Address tujuan, atau mengarahkan koneksi ke localhost.

dst-nat: Kita bisa mengganti IP Address dan port tujuan dari suatu koneksi.

Redirect: Untuk mengalihkan koneksi yang tadinya melwati router, dan dialihkan menuju ke localhost.

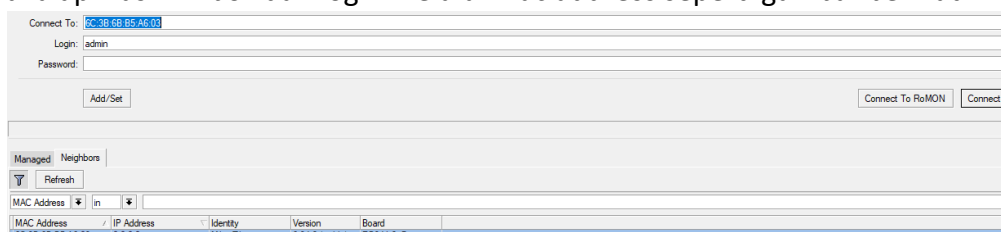
4. Prosedur dan teknik konfigurasi Firewall Jaringan

Dalam konfigurasi firewall jaringan ini, perangkat yang digunakan adalah router board mikrotik 750RB, PC desktop dan Laptop dan/atau android, serta kabel UTP straight secukupnya. Prasyarat dalam mengkonfigurasi firewall, peserta didik telah mampu membuat gateway internet (NAT) pada port either 2.

Konfigurasi firewall ini adalah untuk membuat pembatasan pada either 3 yang akan disambungkan dengan Access Point. Bahwa client yang tersambung melalui Access Point tidak bisa mengakses youtube.

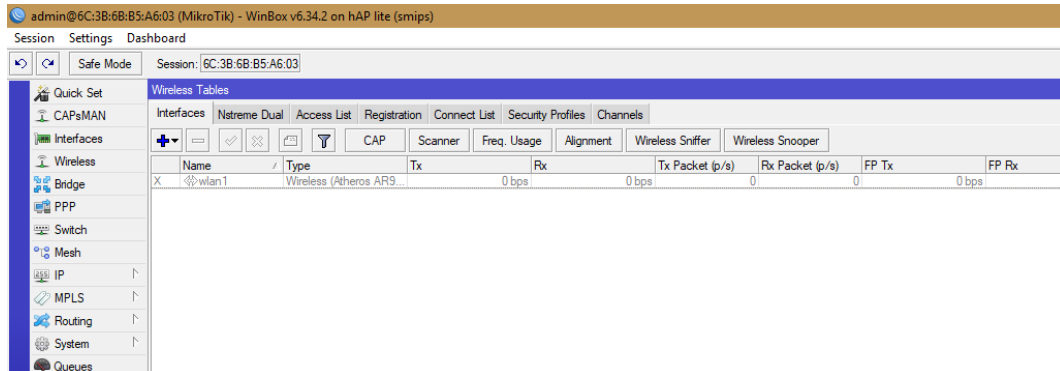
Langkah-langkah konfigurasi firewall dengan Protocol Layer 7 tersebut adalah sebagai berikut:

1. Pastikan pemasangan kabel UTP ke ISP dan ke PC untuk konfigurasi terpasang dengan benar(Ether 1 ke ISP, Ether 2 ke Komputer / Laptop)
2. Buka aplikasi winbox dan login melalui mac address seperti gambar berikut

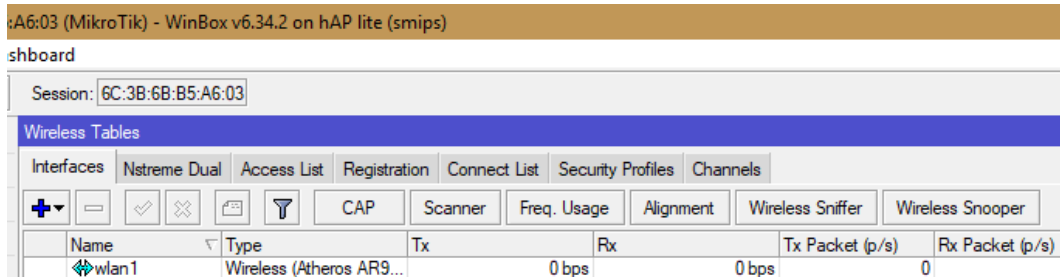
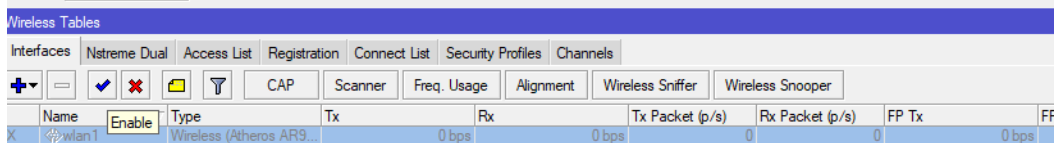


Login dengan user dan password yang telah diberikan pada saat membuat internet gateway (NAT)

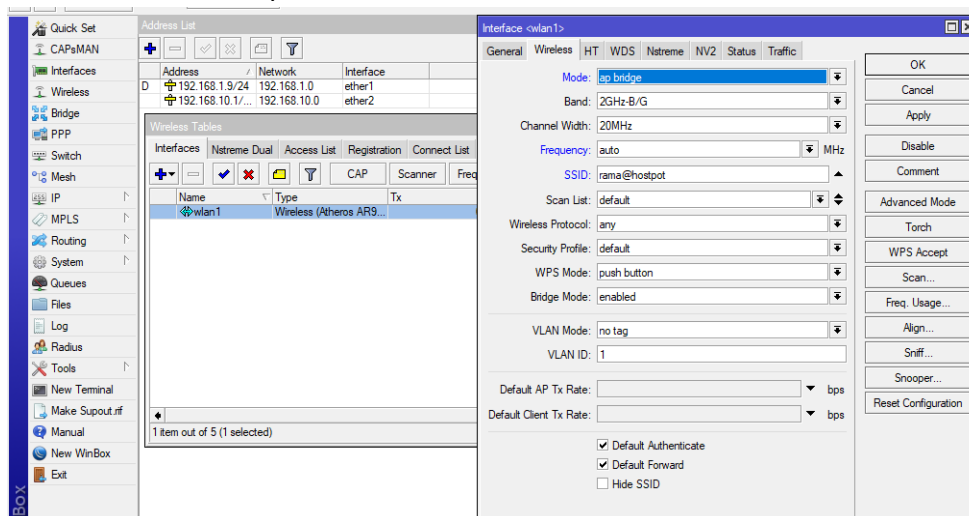
- Setelah masuk winbox pastikan semua konfigurasi internet gateway (NAT) (setting dasar) telah berjalan dengan baik melalui port either 2 mikrotik RB 750.
- Mengaktifkan Wireless dan membuka Wlan1 pada menu Wireless Buka Wireless



Mengaktifkan Wireless Wlan 1 dengan klik centang atau enable berwarna biru

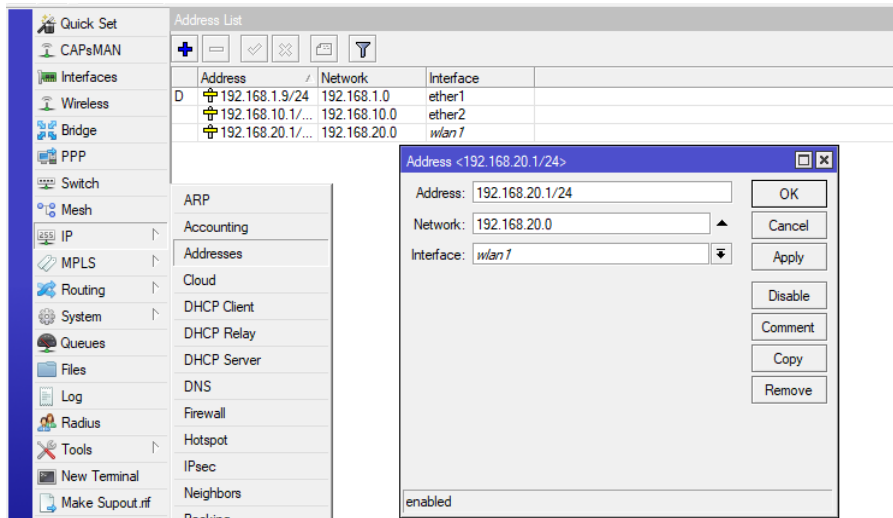


Klik 2 x pada wlan 1 untuk membuka settingan wireless Lalu setting
Mode : AP Bridge Channel Width : 20 Mhz Frequency : Auto
SSID : Hostpot Lab 2 TKJ.

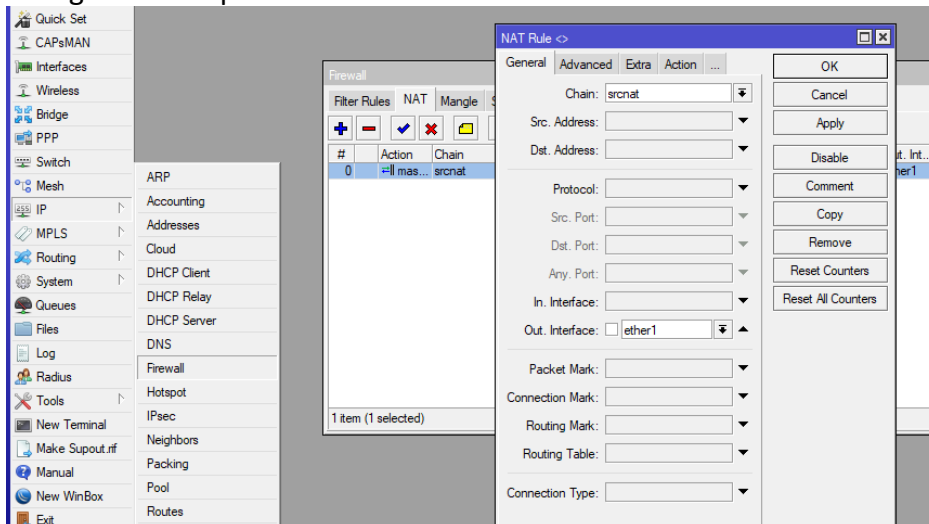


Lalu klik Apply > OK

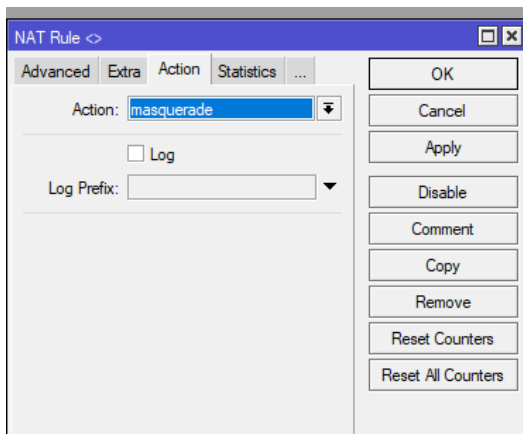
5. Buat IP Address di ether 3 untuk WLAN 1 (192.168.20.1/24) di IP > Addressess dan klik + lalu isi IP dan ganti interface ke WLAN 1 lalu klik Apply > OK



6. Konfigurasi Masquerade : Klik IP > Firewall > NAT

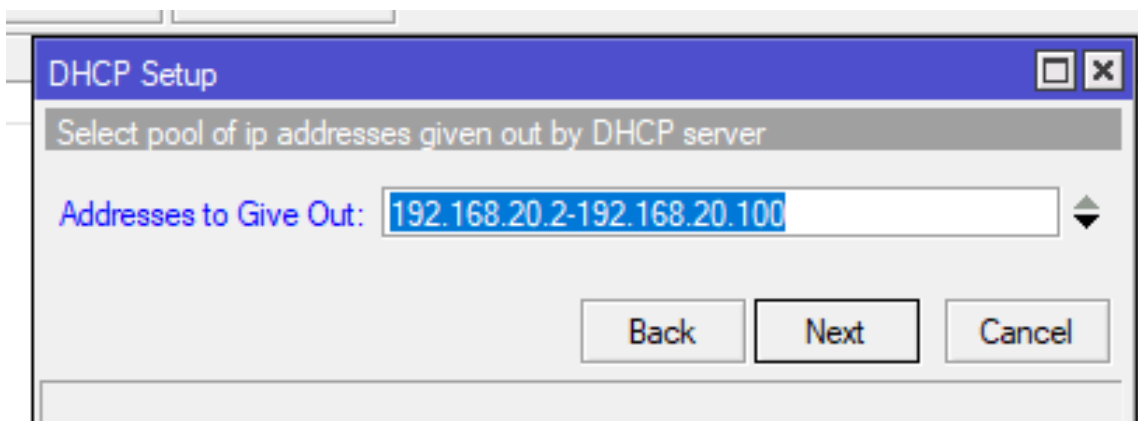
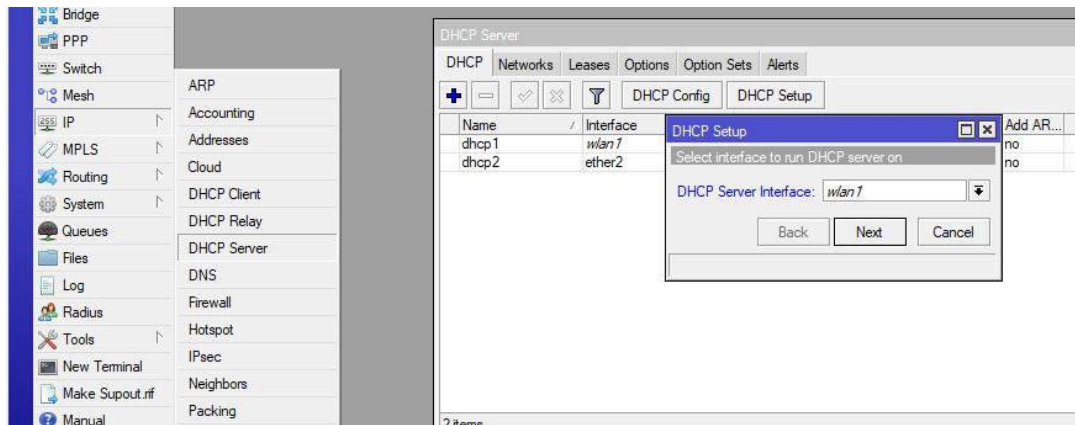


Tambahkan Rule dengan cara klik + > pada tab General > biarkan Chain : srcnat > tambahkan Out Interface dan pilih interface yang mengarah ke ISP / Internet > masuk ke tab action



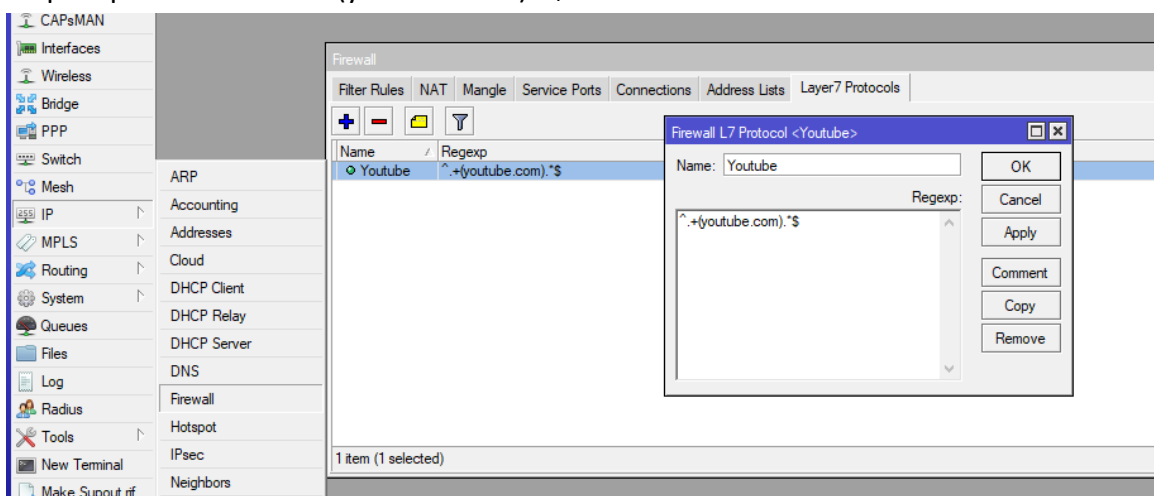
Pilih action > ganti menjadi > masquerade lalu klik Apply > OK

7. Buat DHCP Server pada WLAN 1 agar Wireless dapat memberikan IP secara otomatis pada Client. Klik IP > DHCP SERVER > klik DHCP SETUP > Pilih wlan1 > Klik Next dan sesuaikan

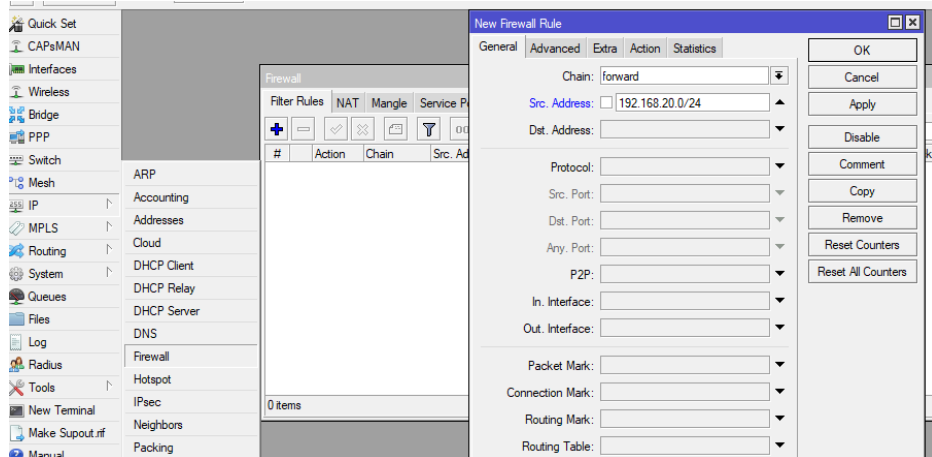


Pada addresses to Give Out sesuaikan dengan soal (IP Pool : 192.168.20.2-192.168.20.100)

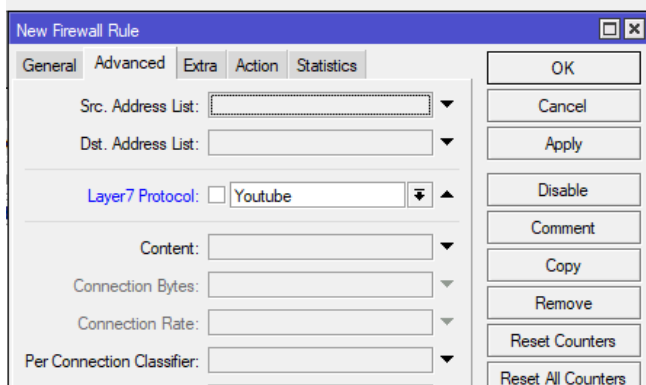
8. Block situs (youtube.com) dengan menggunakan **L7Protocol**. Klik IP > Firewall > L7Protocol > tambahkan rule dengan cara klik + > isi nama (sesuai keinginan) > isikan script seperti berikut : `^(youtube.com).*$`



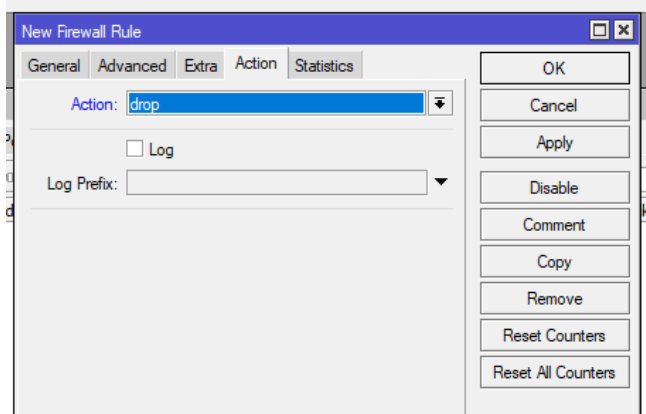
9. Masuk ke tab Filter Rules > lalu tambahkan rules > Chain : Forward > Src. Address : jaringan yang akan diberikan rule (192.168.20.0/24) >



Masuk ke tab Advanced > pada menu Layer7Protocol diaktifkan dan dipilih sesuai yang diisi pada tab Layer7 Protocol (youtube)



Lalu pilih tab Action > pada menu Action pilih drop > klik Apply > OK

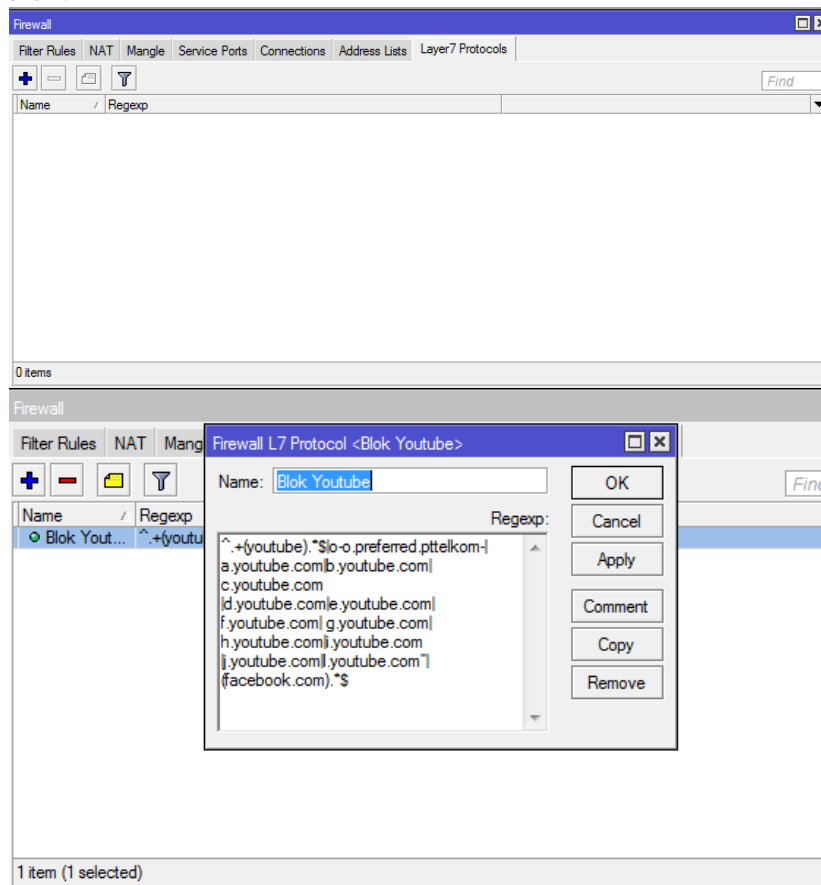


10. Klik menu IP, pilih Firewall, pilih Layer 7 Protocols. Klik add “+” , Buat penamaannya “Blok Youtube”.

Masukkan Regexp dibawah ini :

```
^.(youtube).*[o-o.preferred.pttelkom-  
|a.youtube.com|b.youtube.com|c.youtube.com  
|d.youtube.com|e.youtube.com|f.youtube.com| g.youtube.com|h.youtube.com|i.youtub  
e.com  
|j.youtube.com|l.youtube.com”|(facebook.com).*$
```

Regexp merupakan scripting yang digunakan untuk menambah konten/situs yang akan di blok.



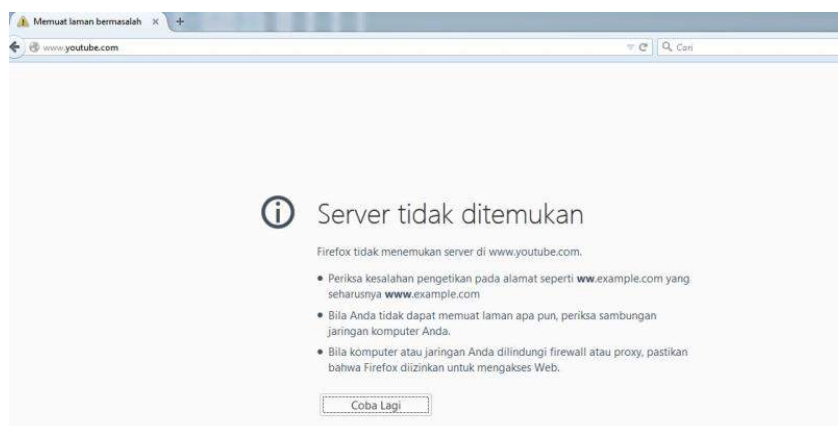
11. Reboot mikrotik router board, dengan cara klik menu System > Reboot.

5. Pengujian hasil konfigurasi **Firewall Jaringan**

Pengujian dilaksanakan setelah dilakukan konfigurasi firewall. Pengujian dilakukan dengan menggunakan laptop atau HP android.

Langkah-langkah pengujian hasil konfigurasi firewall jaringan adalah sebagai berikut:

- Konfigurasi IP address pada laptop/android adalah obtain karena telah dilakukan pengaturan DHCP pada either 3 (hospot)
- Sambungkan Laptop atau Android melalui hossipot Wifi Lab 2 TKJ.
- Buka browser Chrome ketikkan youtube pada url link nya. Kemudian jalankan



- Ketika PC melakukan akses ke <http://www.youtube.com> pada web browser, yang hasilnya

situs tersebut sudah tidak bisa diakses lagi.

C. Penutup

1. Rangkuman

1. Firewall didefinisikan sebagai suatu cara atau mekanisme yang diterapkan baik terhadap hardware, software ataupun system itu sendiri dengan tujuan untuk melindungi, baik dengan menyaring, membatasi atau bahkan menolak suatu atau semua hubungan/kegiatan suatu segmen pada jaringan pribadi dengan jaringan luar yang bukan merupakan ruang lingkungannya.
2. Jenis-jenis Firewall :
 - a. *Packet Filtering Gateway* : firewall yang bertugas melakukan filterisasi terhadap paket-paket yang datang dari luar jaringan yang dilindunginya.
 - b. *Application Layer Gateway*: adalah paket tersebut tidak akan secara langsung sampai ke server tujuan, akan tetapi hanya sampai firewall saja. Selbihnya firewall ini akan membuka koneksi baru ke server tujuan setelah paket tersebut diperiksa berdasarkan aturan yang berlaku.
 - c. *Circuit Level Gateway*: firewall ini bekerja pada bagian Lapisan Transport model referensi TCP/IP. Firewall ini akan melakukan pengawasan terhadap awal hubungan TCP yang biasa disebut sebagai TCP Handshaking, yaitu proses untuk menentukan apakah sesi hubungan tersebut diperbolehkan atau tidak
 - d. *Statefull Multilayer Inspection Firewall*: Firewall jenis ini akan bekerja pada lapisan Aplikasi, Transport dan Internet. Dengan penggabungan ketiga model firewall yaitu Packet Filtering Gateway, Application Layer Gateway dan Circuit Level Gateway, mungkin dapat dikatakan firewall jenis ini merupakan firewall yang,memberikan fitur terbanyak dan memberikan tingkat keamanan yang paling tinggi
3. Fitur Mikrotik Firewall:
 - Rules
 - Nat (source-nat and destination-nat)
 - Mangle
 - Address List
 - Layer 7 Protocol (baru di versi 3)
 - Service Ports
 - Connections
4. Prosedur dan teknik konfigurasi Firewall Jaringan
Dalam konfigurasi firewall jaringan ini, perangkat yang digunakan adalah router board mikrotik 750RB, PC desktop dan Laptop dan/atau android, serta kabel UTP straight secukupnya. Prasyarat dalam mengkonfigurasi firewall, peserta didik telah mampu membuat gateway internet (NAT) pada port either 2. Konfigurasi firewall ini adalah untuk membuat pembatasan pada either 3 yang akan disambungkan dengan Access Point. Bahwa client yang tersambung melalui Access Point tidak bisa mengakses youtube.
5. Pengujian hasil konfigurasi Firewall Jaringan.
Pengujian dilaksanakan setelah dilakukan konfigurasi firewall. Pengujian dilakukan dengan menggunakan laptop atau HP android.

2. Tes Formatif

1. Firewall didefinisikan sebagai suatu cara atau mekanisme yang diterapkan baik terhadap hardware, software ataupun system itu sendiri dengan tujuan untuk melindungi, baik dengan menyaring, membatasi atau bahkan menolak suatu atau semua hubungan/kegiatan suatu segmen pada jaringan pribadi dengan jaringan luar yang bukan merupakan ruang lingkungannya. Pembatasan terhadap suatu segmen pada jaringan antara lain....

- A. Terhadap web Youtube
- B. Terhadap web detik
- C. Terhadap web yahoo
- D. Terhadap web linux
- E. **Semua jawaban benar**

2. Perhatikan proses yang terjadi pada firewall berikut :

- 1. Modifikasi header paket,
- 2. Translasi alamat jaringan, dan
- 3. Filter paket

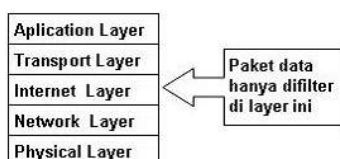
Proses yang digunakan untuk memodifikasi kualitas layanan bit paket TCP sebelum mengalami proses routing terdapat pada nomor...

- A. **Nomor 1.**
- B. Nomor 2
- C. Nomor 3
- D. Nomor 1 dan 2.
- E. Nomor 1 dan 3.

3. 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 berkaitan dengan hardware (pengamanan fisik, sumber daya listrik) maupun yang berkaitan dengan software (sistem, konfigurasi, sistem akses, dll). Pernyataan yang kurang tepat dibawah ini terletak pada.....

- A. Gangguan pada sistem dapat terjadi karena faktor ketidaksengajaan
- B. Gangguan pada sistem dapat terjadi karena faktor disengaja orang lain
- C. Gangguan pada sistem dapat terjadi karena factor human error
- D. **Gangguan pada sistem dapat terjadi karena factor cuaca**
- E. Gangguan pada sistem dapat terjadi karena factor system yang rusak karena penyusunan orang tidak dikenal.

4. Perhatikan gambar berikut ini:

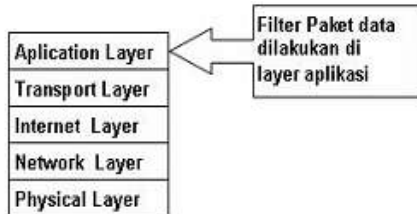


Filterisasi paket ini hanya terbatas pada sumber paket, tujuan paket, dan atribut-atribut dari paket tersebut, misalnya paket tersebut bertujuan ke server kita yang menggunakan alamat IP 202.51.226.35 dengan port 80. Port 80 adalah atribut yang dimiliki oleh paket tersebut. Ini adalah jenis firewall...

A. Packet Filtering Gateway

- B. Packet Filtering data
- C. Application Layer Gateway
- D. Circuit Level Gateway
- E. Statefull Multilayer Inspection Firewall

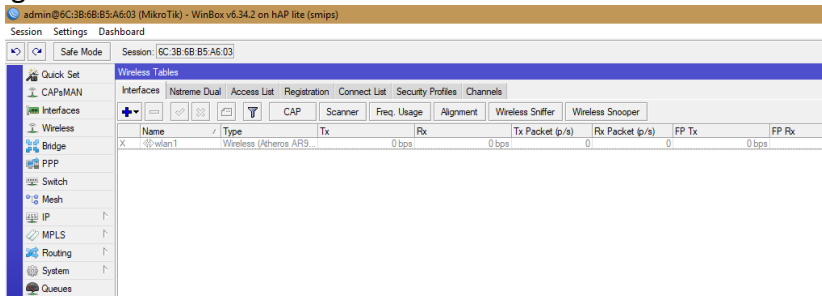
5. Perhatikan gambar berikut ini:



Mekanisme lainnya yang terjadi adalah paket tersebut tidak akan secara langsung sampai ke server tujuan, akan tetapi hanya sampai firewall saja. Selebihnya firewall ini akan membuka koneksi baru ke server tujuan setelah paket tersebut diperiksa berdasarkan aturan yang berlaku. Bila kita melihat dari sisi layer TCP/IP, firewall jenis ini akan melakukan filterisasi pada layer aplikasi (Application Layer. Ini adalah jenis firewall...

- A. Packet Filtering Gateway
 - B. Packet Filtering data
 - C. Application Layer Gateway**
 - D. Circuit Level Gateway
 - E. Statefull Multilayer Inspection Firewall
6. Model firewall ini bekerja pada bagian Lapisan Transport model referensi TCP/IP. Firewall ini akan melakukan pengawasan terhadap awal hubungan TCP yang biasa disebut sebagai TCP Handshaking, yaitu proses untuk menentukan apakah sesi hubungan tersebut diperbolehkan atau tidak. Bentuknya hampir sama dengan Application Layer Gateway, hanya saja bagian yang difilter terdapat ada lapisan yang berbeda, yaitu berada pada layer Transport. Ini adalah jenis firewall adalah...
- A. Packet Filtering Gateway
 - B. Packet Filtering data
 - C. Application Layer Gateway
 - D. Circuit Level Gateway**
 - E. Statefull Multilayer Inspection Firewall
7. Sistem yang menampilkan informasi statistik akan besar atau banyaknya paket-paket yang melewati sebuah router. Maka dengan fitur ini kita bisa melakukan monitoring terhadap sebuah jaringan dan memungkinkan bagi kita untuk mengidentifikasi berbagai macam masalah yang terjadi di dalamnya. Selain itu, dengan memanfaatkan fitur ini kita dapat melakukan analisa dan meningkatkan performa dari router. Dari daftar diatas, Sistem monitor pada firewall yang diterapkan pada system jaringan ini adalah..
- A. Simple Packet Flow
 - B. Connection Tracking.
 - C. Connection tracking
 - D. Implikasi Connection State.
 - E. Traffic Flow**

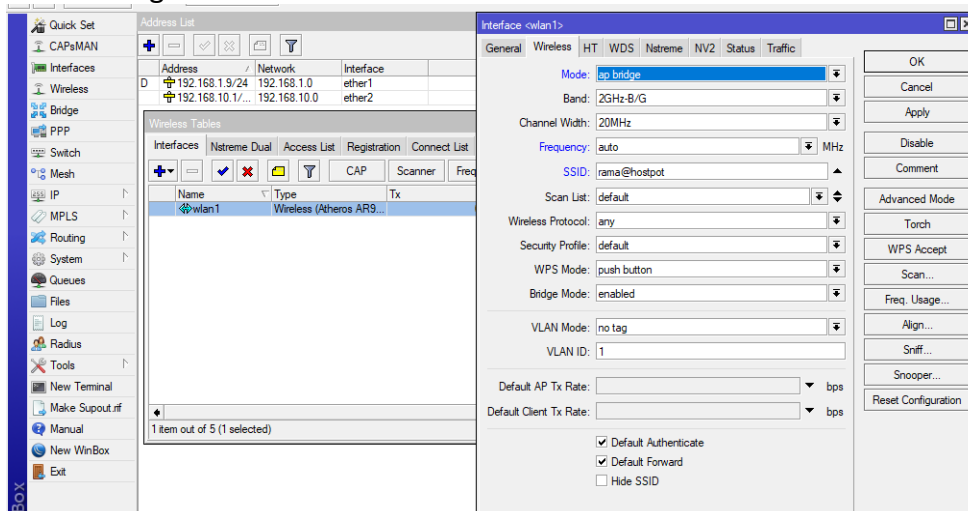
8. Pada menu Wireless, klik centang atau enable berwarna biru sseperti yang Nampak pada gambar berikut:



Langkah konfigurasi ini adalah

- A. Konfigurasi Wireless untuk membuat profil password
- B. Konfigurasi Wireless untuk membuat nama wifi
- C. Konfigurasi Wireless untuk membuat repeater
- D. **Mengaktifkan Wireless untuk menuju ke langkah berikutnya**
- E. Mengaktifkan Wireless untuk memberikan IP address

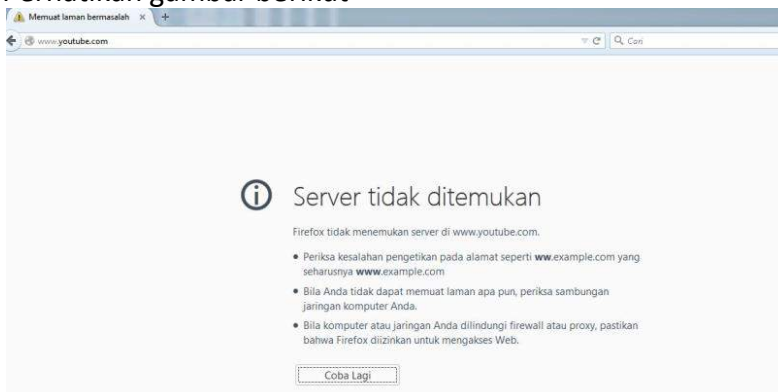
9. Perhatikan gambar berikut



Langkah konfigurasi ini adalah..

- A. Konfigurasi Wireless untuk membuat profil password
- B. **Konfigurasi Wireless untuk membuat nama wifi**
- C. Konfigurasi Wireless untuk membuat repeater
- D. Mengaktifkan Wireless untuk menuju ke langkah berikutnya
- E. Mengaktifkan Wireless untuk memberikan IP address.

10. Perhatikan gambar berikut



Hasil pengujian konfigurasi firewall untuk membatasi PC Client terhadap web youtube, jika kita ping www.youtube dari CMD client, maka tampilan di cmd adalah...

- A. Request Time Out
- B. ReplyTTL
- C. **Destination Host Unreachable**
- D. General Failure
- E. Semua salah

Daftar Pustaka

1. Riadi, I. (2011). *Optimalisasi Keamanan Jaringan Menggunakan Pemfilteran Aplikasi Berbasis Mikrotik*. JUSI Vol. 1, No. 1 , 74.
2. Tomy Alif Mustofa¹ , Edhy Sutanta² , Joko Triyono³ Jurnal JARKOM Vol. 7 No. 2 Desember 2019: *PERANCANGAN DAN IMPLEMENTASI SISTEM MONITORING JARINGAN WI-FI MENGGUNAKAN MIKHMOM ONLINE DI WISMA MUSLIM KLITREN GONDOKUSUMAN YOGYAKARTA*, Program Studi Informatika, Fakultas Teknologi Industri Institut Sains & Teknologi AKPRIND Yogyakarta
3. Video Youtube: konsep dan jenis firewall, link :
<https://www.youtube.com/watch?v=fET2PYkckLo&t=88s>
4. Video Youtube: konfigurasi jaringan nirkabel, link:
https://www.youtube.com/watch?v=9Va9sLJE_0Q

Kunci Jawaban Test Formatif

1. E
2. A
3. D
4. A
5. C
6. D
7. E
8. D
9. B
10. C

Nama : Sujarwoko
Kelas : *TIK , A, Angkatan 3 Tahun 2021*
LPPT: Universitas Sebelas Maret

Sekolah : SMK Binawiyata Karangmalang Sragen
Kelas/Semester : XII TKJ / 5
Mata pelajaran : Administrasi Infrastruktur Jaringan (AIJ)
Materi Pembelajaran: Firewall Jaringan

Materi:

- ✓ *Firewall Jaringan*
- ✓ *Prosedur dan langkah konfigurasi Firewall Jaringan*
- ✓ *Pengujian Hasil konfigurasi Firewall Jaringan*

Kompetensi Dasar

3.10 Mengevaluasi Firewall Jaringan

4.10 Mengkonfigurasi Firewall Jaringan

Indikator Pencapaian Kompetensi

3.10.1 Mengidentifikasi tentang firewall jaringan

3.10.2 Menganalisis jenis firewall jaringan

3.10.3 Memilih prosedur dan teknik konfigurasi firewall jaringan (C5)

4.10.1 Melakukan konfigurasi *firewall* jaringan (P5)

4.10.2 Menguji hasil konfigurasi *firewall* jaringan (P5)

Tujuan Pembelajaran

1. Peserta didik (A) dapat **mengidentifikasi** tentang *firewall* jaringan (B) setelah membaca Power point dan melihat literatur *firewall* jaringan (C) dengan tepat dan mandiri (D)
2. Peserta didik (A) mampu **menganalisis** jenis *firewall* jaringan (B) melalui tayangan video *firewall* jaringan (C) dengan tepat dan mandiri (D)
3. Peserta didik (A) mampu **memilih** prosedur dan teknik konfigurasi *firewall* jaringan (B) melalui tayangan video *firewall* jaringan (C) dengan percaya diri dan tanggung jawab (D)
4. Peserta didik (A) mampu **mengkonfigurasi** *firewall* jaringan (B) setelah berdiskusi tentang prosedur dan teknik konfigurasi *firewall* jaringan (C) dengan percaya diri dan tanggung jawab (D)
5. Peserta didik (A) mampu **menguji** hasil konfigurasi *firewall* jaringan (B) setelah berdiskusi tentang menguji hasil konfigurasi *firewall* jaringan (C) dengan percaya diri dan tanggung jawab (D)

A= Audience; B= Behaviour; C= Condition; D= Degree

Studi Kasus Firewall Jaringan

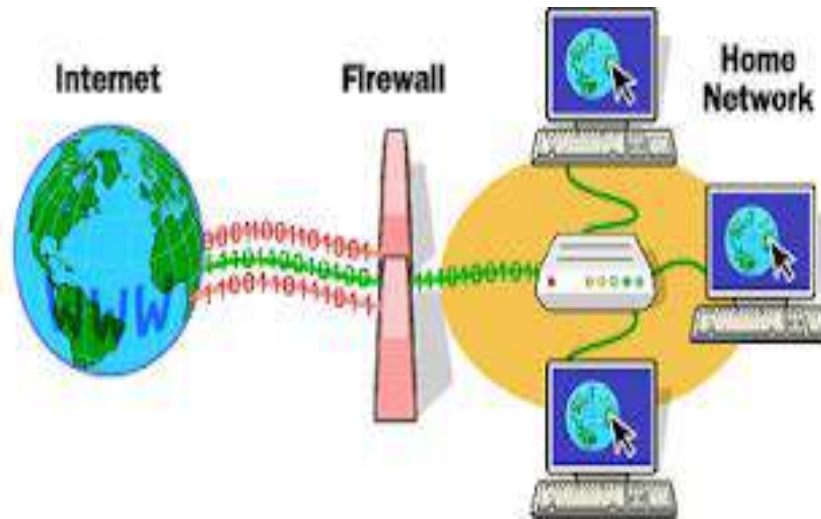
Di Lab 2 TKJ SMK Binawiyata ini, setiap siswa secara bebas bisa mengakses youtube melalui androidnya tanpa ada pembatasan. Hal ini akan sangat mengganggu konsentrasi siswa di saat pembelajaran desain.

- ❖ diperlukan pembatasan akses, agar siswa dapat focus dengan pembelajaran yang sedang berlangsung
- ❖ maka diperlukan sebuah firewall jaringan yang dikonfigurasi sesuai dengan kebutuhan.

Dalam membangun firewall jaringan

- Diperlukan mikrotik router board yang dikonfigurasi dengan cara yang benar dan efisien

Firewall Jaringan



- ✓ sebagai suatu cara atau mekanisme yang diterapkan baik terhadap hardware, software ataupun system itu sendiri dengan tujuan untuk melindungi, baik dengan menyaring, membatasi atau bahkan menolak suatu atau semua hubungan/kegiatan suatu segmen pada jaringan pribadi dengan jaringan luar yang bukan merupakan ruang lingkungannya.

Proses yang terjadi pada firewall

✓ Modifikasi header paket.

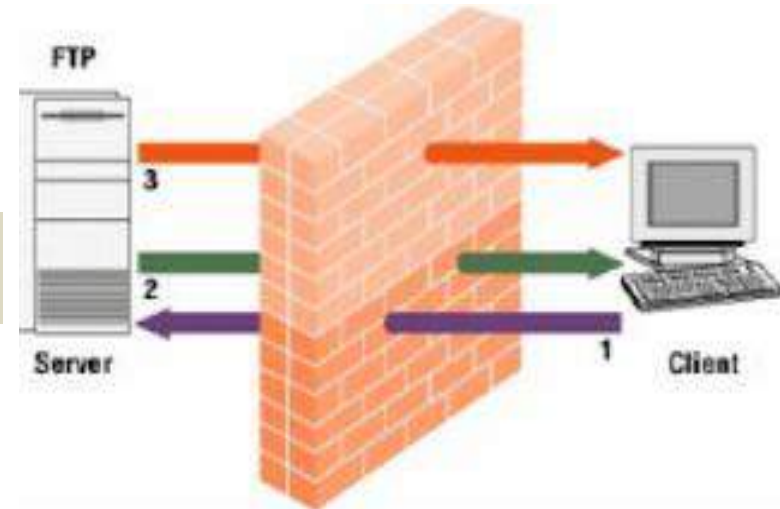
digunakan untuk memodifikasi kualitas layanan bit paket TCP sebelum mengalami proses routing

✓ Translasi alamat jaringan

Translasi yang terjadi dapat berupa translasi satu ke satu (one to one), yaitu satu alamat IP privat dipetakan kesatu alamat IP publik atau translasi banyak kesatu (many to one)

✓ Filter paket

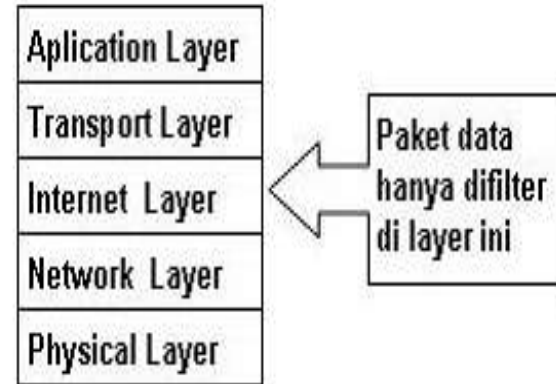
Digunakan untuk menentukan nasib paket apakah dapat diteruskan atau tidak



Jenis-jenis Firewall (1)

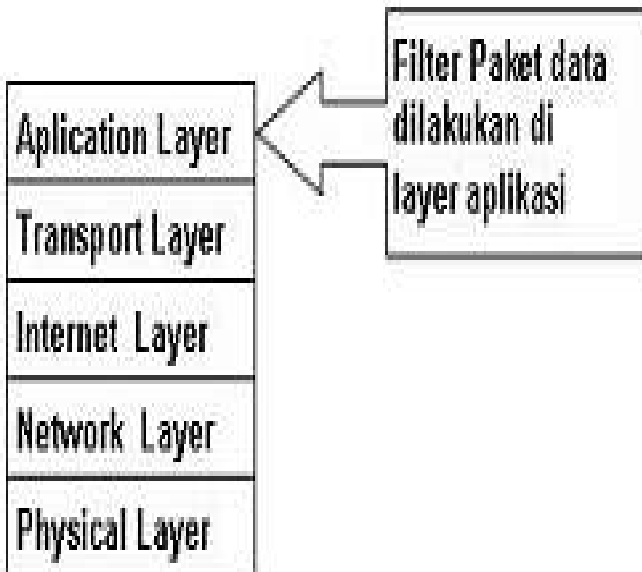
1. Packet Filtering Gateway

- firewall yang bertugas melakukan filterisasi terhadap paket-paket yang datang dari luar jaringan yang dilindunginya
- firewall ini akan bekerja pada layer internet



2. Application Layer Gateway

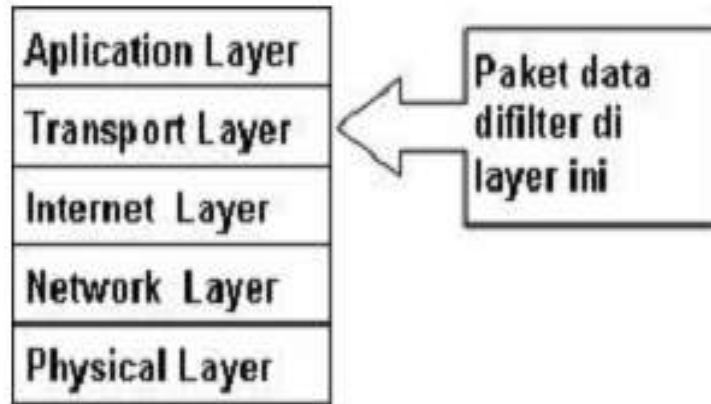
- adalah paket tersebut tidak akan secara langsung sampai ke server tujuan, akan tetapi hanya sampai firewall saja
- Selebihnya firewall ini akan membuka koneksi baru ke server tujuan setelah paket tersebut diperiksa berdasarkan aturan yang berlaku



Jenis-jenis Firewall (2)

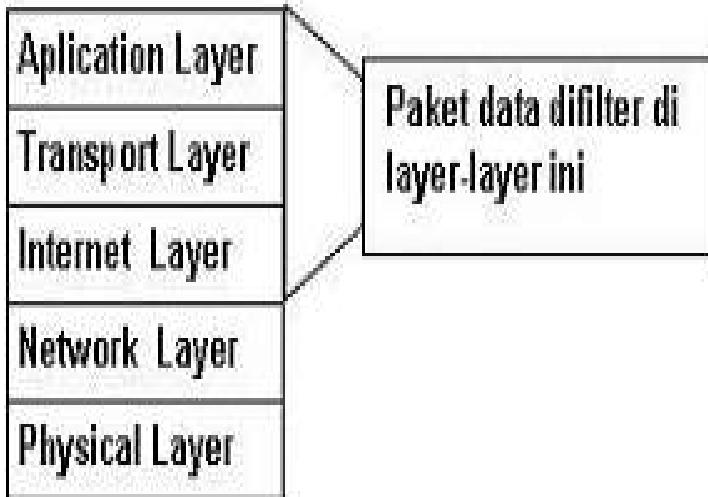
3. Circuit Level Gateway

- akan melakukan pengawasan terhadap awal hubungan TCP yang biasa disebut sebagai TCP Handshaking
- bekerja pada bagian Lapisan Transport model referensi TCP/IP



4. Statefull Multilayer Inspection Firewall

- merupakan penggabungan dari ketiga firewall sebelumnya
- bekerja pada lapisan Aplikasi, Transport dan Internet



Fitur Mikrotik Firewall (1)

fitur firewall yang berfungsi untuk melindungi dengan cara mendrop atau mengaccept sebuah paket yang akan masuk, melewati, atau keluar router

➤ Rules.

Filter rules untuk melakukan kebijakan boleh atau tidaknya sebuah trafik ada dalam jaringan, identik dengan accept atau drop

➤ Nat (source-nat and destination-nat)

NAT digunakan untuk melakukan perubahan baik src-address ataupun dst-address

➤ Mangle

adalah cara untuk menandai paket-paket data tertentu, dan kita akan menggunakan tanda tersebut pada fitur lainnya, misalnya pada filter, routing, NAT, ataupun queue

➤ Address List

Address-list digunakan untuk memfilter group IP address dengan 1 rule firewall

➤ Layer 7 Protocol (baru di versi 3)

merupakan fitur yang digunakan untuk menentukan metode pencarian pola terhadap paket data yang melewati jalur ICMP, TCP, dan UDP Atau istilah lainnya regex pattern. Biasanya digunakan untuk melakukan blocking terhadap situs web dengan SSL “https://”

➤ Service Ports

merupakan fitur yang digunakan untuk menonaktifkan atau merubah port-port yang aktif

➤ Connections

- *Connection Tracking* : adalah “jantung” dari firewall, mengumpulkan informasi tentang active connections. Dengan mendisable connection tracking router akan kehilangan fungsi NAT, filter rule dan mangle
- *Connection State*: proses filtering hanya dilakukan pada saat connection dimulai (connection-state=new).

Prosedur dan teknik konfigurasi *Firewall Jaringan* (1)

Konfigurasi firewall ini adalah untuk membuat pembatasan pada either 3 yang akan disambungkan dengan Access Point. Bahwa client yang tersambung melalui Access Point tidak bisa mengakses youtube.

Perangkat yang digunakan adalah

- Routerboard mikrotik 750RB
- PC desktop dan Laptop/Android
- Kabel UTP straight

- ✓ Pastikan pemasangan kabel UTP ke ISP dan ke PC untuk konfigurasi terpasang dengan benar (Ether 1 ke ISP, Ether 2 ke Komputer / Laptop)
- ✓ Buka aplikasi winbox dan login melalui mac address seperti gambar berikut
- ✓ Login dengan user dan password yang telah diberikan pada saat membuat internet gateway (NAT)

Connect To: 6C:3B:6B:B5:A6:03

Login: admin

Password:

Add/Set

Connect To RoMON

Connect

Managed Neighbors

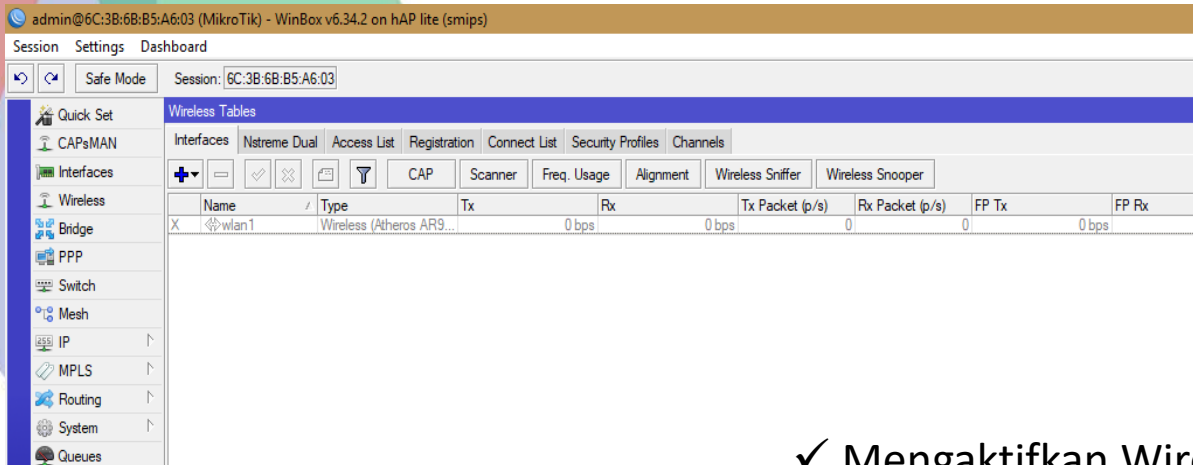
Refresh

MAC Address in

MAC Address	IP Address	Identity	Version	Board
6C:3B:6B:B5:A6:03	0.0.0.0	MikroTik	6.34.2 (stable)	RB941-2nD

Prosedur dan teknik konfigurasi *Firewall Jaringan* (2)

- ✓ Setelah masuk winbox pastikan semua konfigurasi internet gateway (NAT) (setting dasar) telah berjalan dengan baik melalui port ether 2 mikrotik RB 750.
- ✓ Mengaktifkan Wireless dan membuka Wlan1 pada menu Wireless Buka Wireless



admin@6C:3B:6B:B5:A6:03 (MikroTik) - WinBox v6.34.2 on hAP lite (smips)

Session Settings Dashboard

Safe Mode Session: 6C:3B:6B:B5:A6:03

Wireless Tables

Interfaces Nstreme Dual Access List Registration Connect List Security Profiles Channels

+ - ✓ ✕ CAP Scanner Freq. Usage Alignment Wireless Sniffer Wireless Snooper

Name	Type	Tx	Rx	Tx Packet (p/s)	Rx Packet (p/s)	FP Tx	FP Rx
X wlan1	Wireless (Atheros AR9...	0 bps	0 bps	0	0	0	0 bps

- ✓ Mengaktifkan Wireless Wlan 1 dengan klik centang atau enable berwarna biru

:A6:03 (MikroTik) - WinBox v6.34.2 on hAP lite (smips)

shboard

Session: 6C:3B:6B:B5:A6:03

Wireless Tables

Interfaces Nstreme Dual Access List Registration Connect List Security Profiles Channels

+ - ✓ ✕ CAP Scanner Freq. Usage Alignment Wireless Sniffer Wireless Snooper

Name	Type	Tx	Rx	Tx Packet (p/s)	Rx Packet (p/s)
✓ wlan1	Wireless (Atheros AR9...	0 bps	0 bps	0	0

Prosedur dan teknik konfigurasi *Firewall Jaringan* (3)

- ✓ Klik 2 x pada wlan 1 untuk membuka settingan wireless Lalu setting
Mode : AP Bridge
Channel Width : 20 Mhz
Frequency : Auto
SSID : Hostpot Lab 2 TKJ.
- ✓ Lalu klik Apply > OK

The screenshot displays the Mikrotik WinBox interface. On the left, a sidebar menu shows various configuration categories like Quick Set, CAPsMAN, Interfaces, Wireless, Bridge, PPP, Switch, Mesh, IP, MPLS, Routing, System, Queues, Files, Log, Radius, Tools, New Terminal, Make Supout.tif, Manual, New WinBox, and Exit. The main window is divided into two panes. The top pane, titled 'Address List', shows a table with columns for Address, Network, and Interface. The bottom pane, titled 'Wireless Tables', shows a table with columns for Name, Type, and Tx. The 'Interface <wlan1>' configuration window is open, showing the 'Wireless' tab. The 'Mode' is set to 'ap bridge', 'Band' to '2GHz-B/G', 'Channel Width' to '20MHz', 'Frequency' to 'auto', and 'SSID' to 'rama@hostpot'. The 'General' tab is also visible, showing the interface name 'wlan1' and type 'Wireless (Atheros AR9...)'.

Address	Network	Interface
192.168.1.9/24	192.168.1.0	ether1
192.168.10.1/...	192.168.10.0	ether2

Name	Type	Tx
wlan1	Wireless (Atheros AR9...)	

Interface <wlan1>

General Wireless HT WDS Nstreme NV2 Status Traffic

Mode: ap bridge
Band: 2GHz-B/G
Channel Width: 20MHz
Frequency: auto MHz
SSID: rama@hostpot
Scan List: default
Wireless Protocol: any
Security Profile: default
WPS Mode: push button
Bridge Mode: enabled
VLAN Mode: no tag
VLAN ID: 1
Default AP Tx Rate: bps
Default Client Tx Rate: bps
 Default Authenticate
 Default Forward
 Hide SSID

OK
Cancel
Apply
Disable
Comment
Advanced Mode
Torch
WPS Accept
Scan...
Freq. Usage...
Align...
Sniff...
Snooper...
Reset Configuration

Prosedur dan teknik konfigurasi *Firewall Jaringan* (4)

- ✓ Buat IP Address di ether 3 untuk WLAN 1 (192.168.20.1/24) di IP > Addresess dan klik + lalu isi IP dan ganti interface ke WLAN 1
- ✓ Lalu klik Apply > OK

The screenshot displays the Mikrotik WinBox interface. On the left is a navigation tree with 'IP' selected. The main window shows the 'Address List' configuration page. A table lists existing IP addresses, and a new entry is being added. A dialog box titled 'Address <192.168.20.1/24>' is open, showing the configuration for the new address.

Address	Network	Interface
192.168.1.9/24	192.168.1.0	ether1
192.168.10.1/...	192.168.10.0	ether2
192.168.20.1/...	192.168.20.0	wlan1

Address <192.168.20.1/24>

Address: 192.168.20.1/24
Network: 192.168.20.0
Interface: wlan1

Buttons: OK, Cancel, Apply, Disable, Comment, Copy, Remove

enabled

Prosedur dan teknik konfigurasi *Firewall Jaringan* (5)

✓ Konfigurasi Masquerade : Klik IP > Firewall > NAT

The screenshot displays the Mikrotik WinBox interface. On the left is a navigation tree with 'IP' selected. The main window shows the 'Firewall' configuration page with the 'NAT' tab active. A table lists a single NAT rule:

#	Action	Chain
0	mas...	srcnat

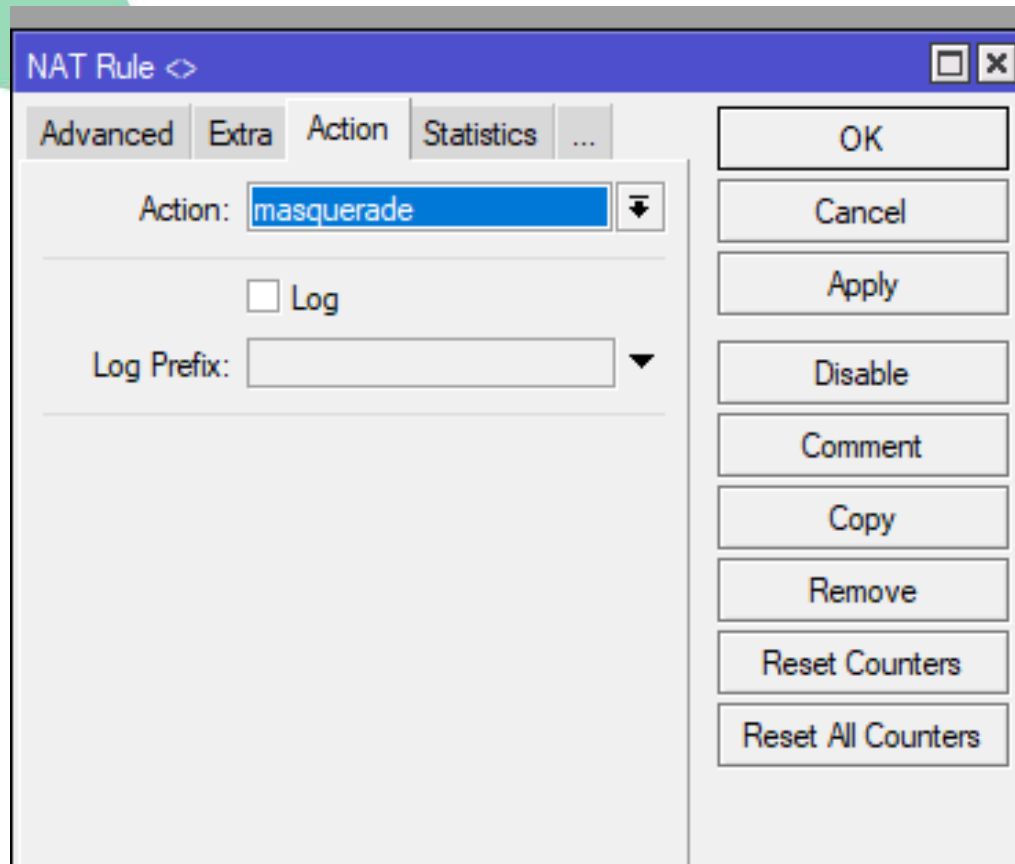
Below the table, it indicates '1 item (1 selected)'. A 'NAT Rule' dialog box is open, showing the configuration for the selected rule:

- Chain: srcnat
- Src. Address: [empty]
- Dst. Address: [empty]
- Protocol: [empty]
- Src. Port: [empty]
- Dst. Port: [empty]
- Any. Port: [empty]
- In. Interface: [empty]
- Out. Interface: ether1
- Packet Mark: [empty]
- Connection Mark: [empty]
- Routing Mark: [empty]
- Routing Table: [empty]
- Connection Type: [empty]

Buttons on the right side of the dialog include OK, Cancel, Apply, Disable, Comment, Copy, Remove, Reset Counters, and Reset All Counters.

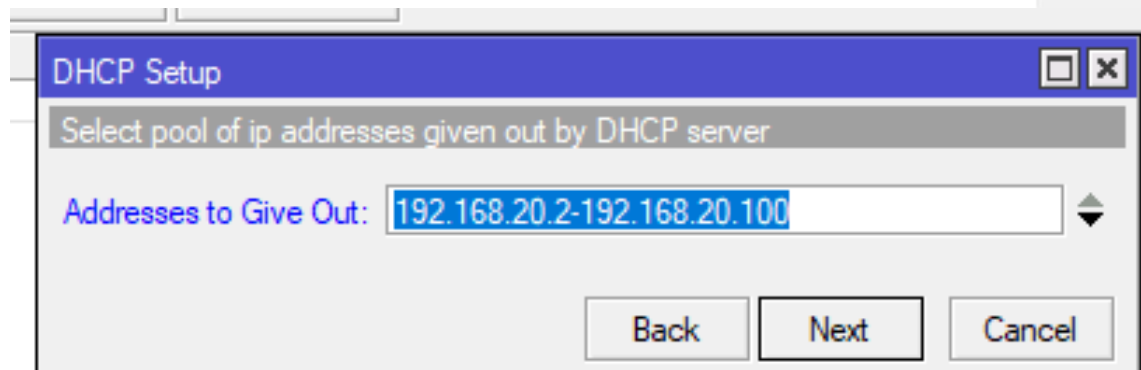
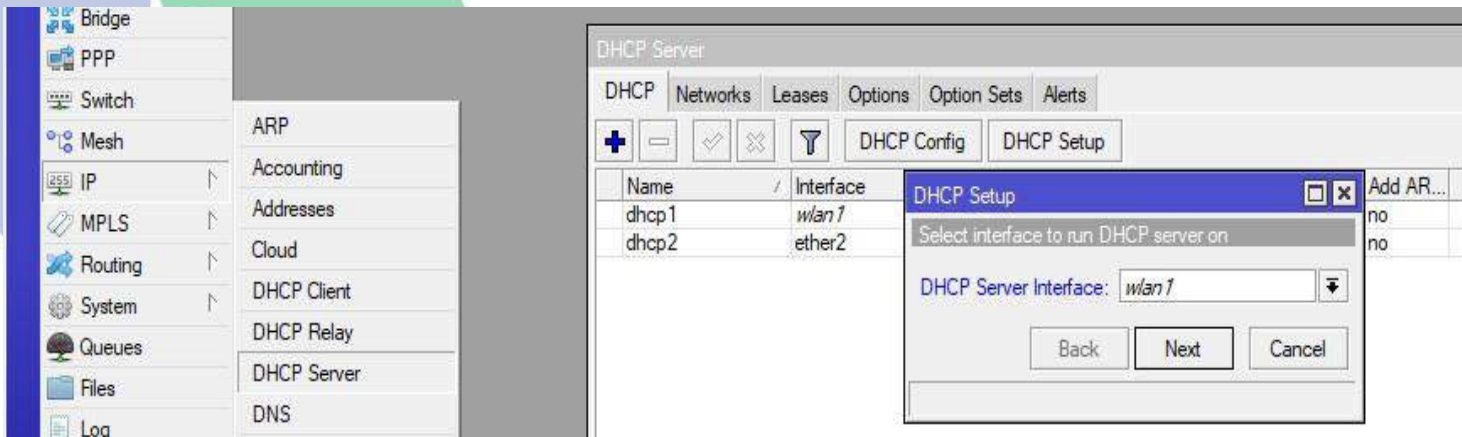
Prosedur dan teknik konfigurasi *Firewall Jaringan* (6)

- ✓ Tambahkan Rule dengan cara klik + > pada tab General > biarkan Chain : srcnat > tambahkan Out Interface dan pilih interface yang mengarah ke ISP / Internet > masuk ke tab action
- ✓ Pilih action > ganti menjadi > masquerade lalu klik Apply > OK



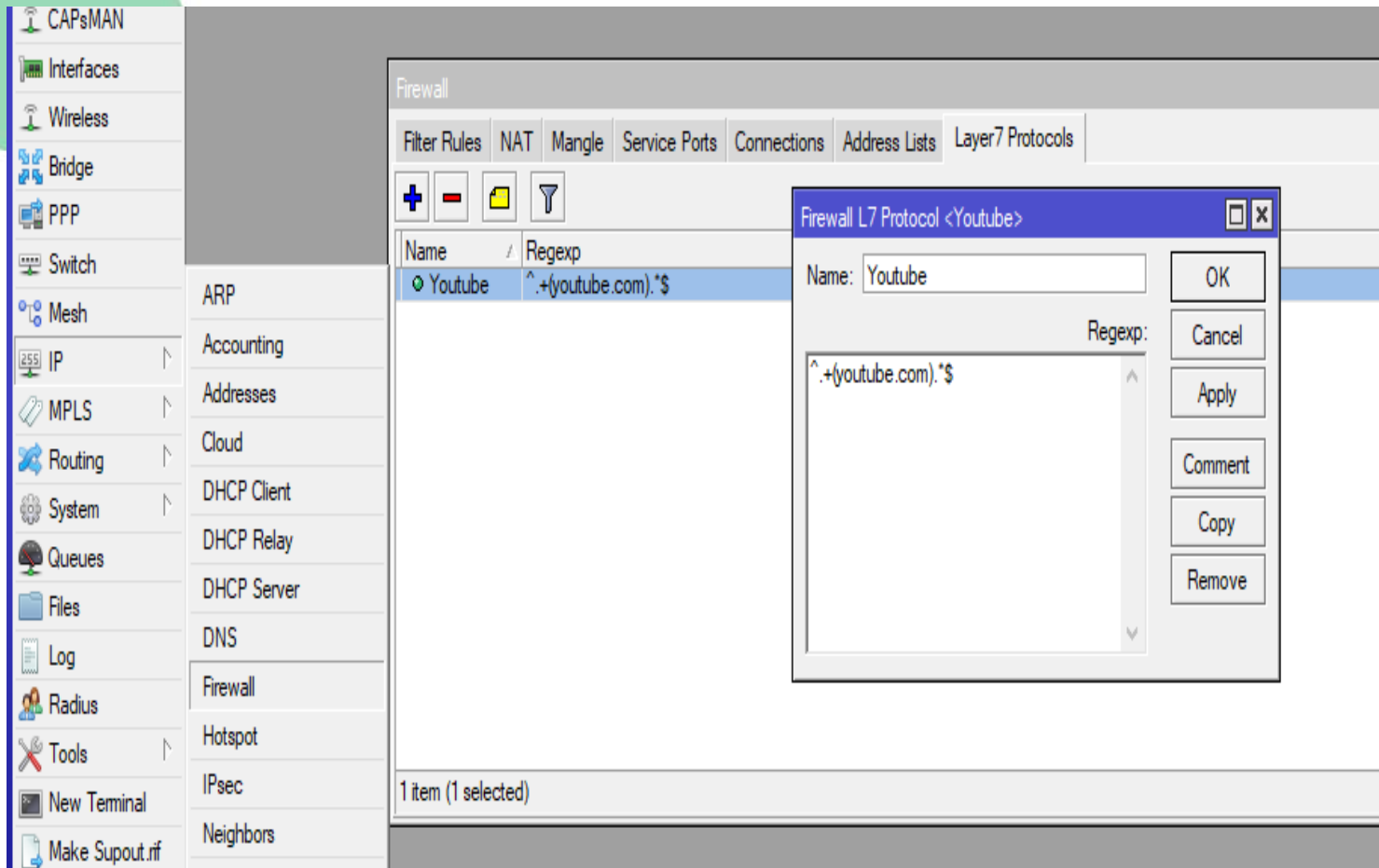
Prosedur dan teknik konfigurasi *Firewall Jaringan* (7)

- ✓ Buat DHCP Server pada WLAN 1 agar Wireless dapat memberikan IP secara otomatis pada Client. Klik IP > DHCP SERVER > klik DHCP SETUP > Pilih wlan1 > Klik Next dan sesuaikan
- ✓ Pada addresses to Give Out sesuaikan dengan soal (IP Pool : 192.168.20.2-192.168.20.100)



Prosedur dan teknik konfigurasi *Firewall Jaringan* (8)

- ✓ Block situs (youtube.com) dengan menggunakan **L7Protocol**. Klik IP > Firewal > L7Protocol > tambahkan rule dengan cara klik + > isi nama (sesuai keinginan) > isikan script seperti berikut : `^.(youtube.com).*$`



Prosedur dan teknik konfigurasi *Firewall Jaringan* (9)

✓ Masuk ke tab Filter Rules > lalu tambahkan rules > Chain : Forward > Src. Address : jaringan yang akan diberikan rule (192.168.20.0/24) >

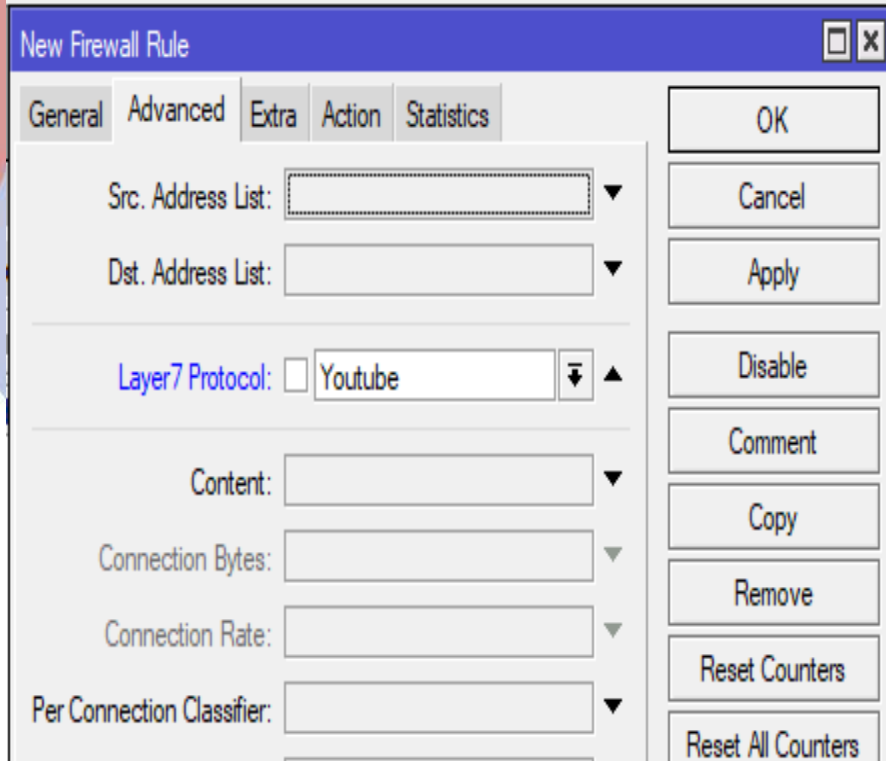
The screenshot displays the Mikrotik WinBox interface for configuring a Firewall Rule. The 'New Firewall Rule' dialog is open, showing the 'General' tab. The 'Chain' is set to 'forward', 'Src. Address' is '192.168.20.0/24', and 'Dst. Address' is empty. The background shows the WinBox interface with the 'Filter Rules' tab selected in the Firewall section.

#	Action	Chain	Src. Ad
0 items			

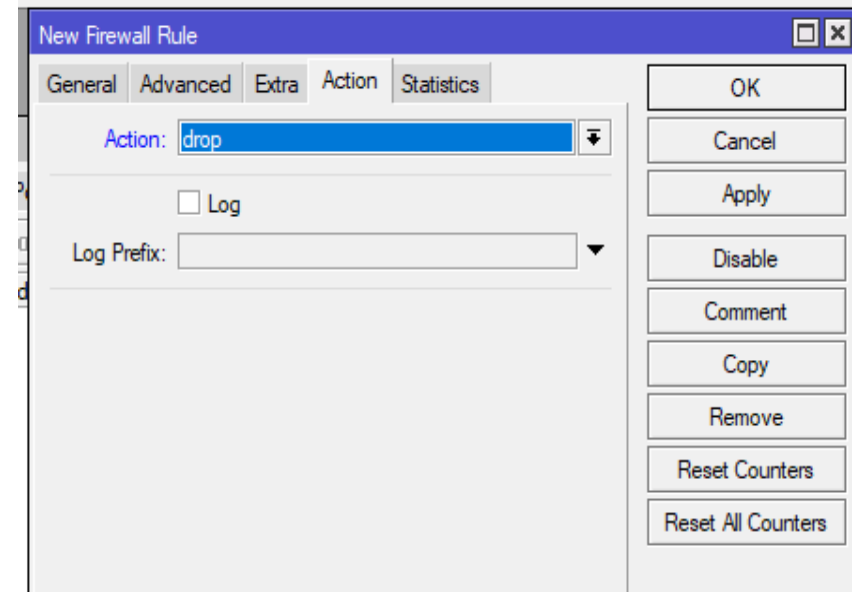
Buttons in the dialog: OK, Cancel, Apply, Disable, Comment, Copy, Remove, Reset Counters, Reset All Counters.

Prosedur dan teknik konfigurasi *Firewall Jaringan* (10)

✓ Masuk ke tab Advanced > pada menu Layer7Protocol diaktifkan dan dipilih sesuai yang diisi pada tab Layer7 Protocol (youtube)

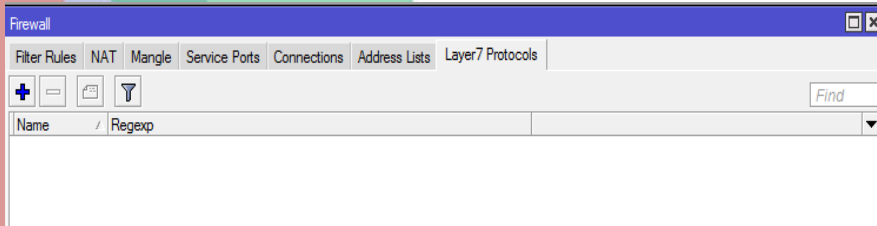


✓ Lalu pilih tab Action > pada menu Action pilih drop > klik Apply > OK



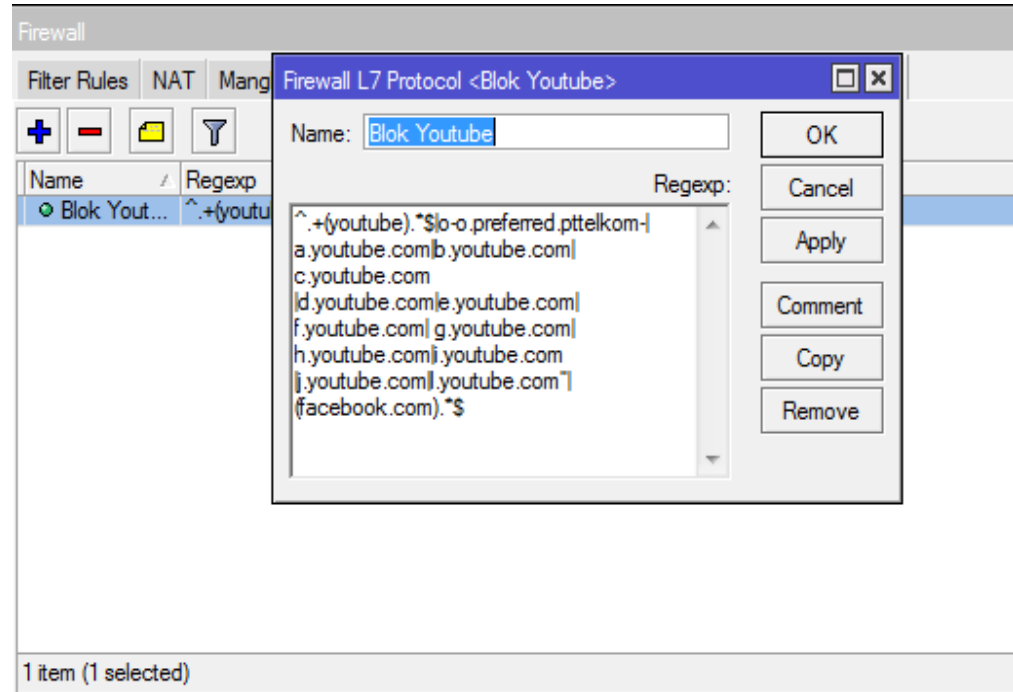
Prosedur dan teknik konfigurasi *Firewall Jaringan* (11)

- ✓ Klik menu **IP**, pilih **Firewall**, pilih **Layer 7 Protocols**. Klik add “+” , Buat penamaannya “Blok Youtube”.



- ✓ Masukkan Regexp dibawah ini :

```
^.+(youtube).*$|o-  
o.preferred.pttelkom-  
|a.youtube.com|b.youtube.com|c.y  
outube.com  
|d.youtube.com|e.youtube.com|f.y  
outube.com|g.youtube.com|h.yout  
ube.com|i.youtube.com  
|j.youtube.com|l.youtube.com”|(fa  
cebook.com).*$
```

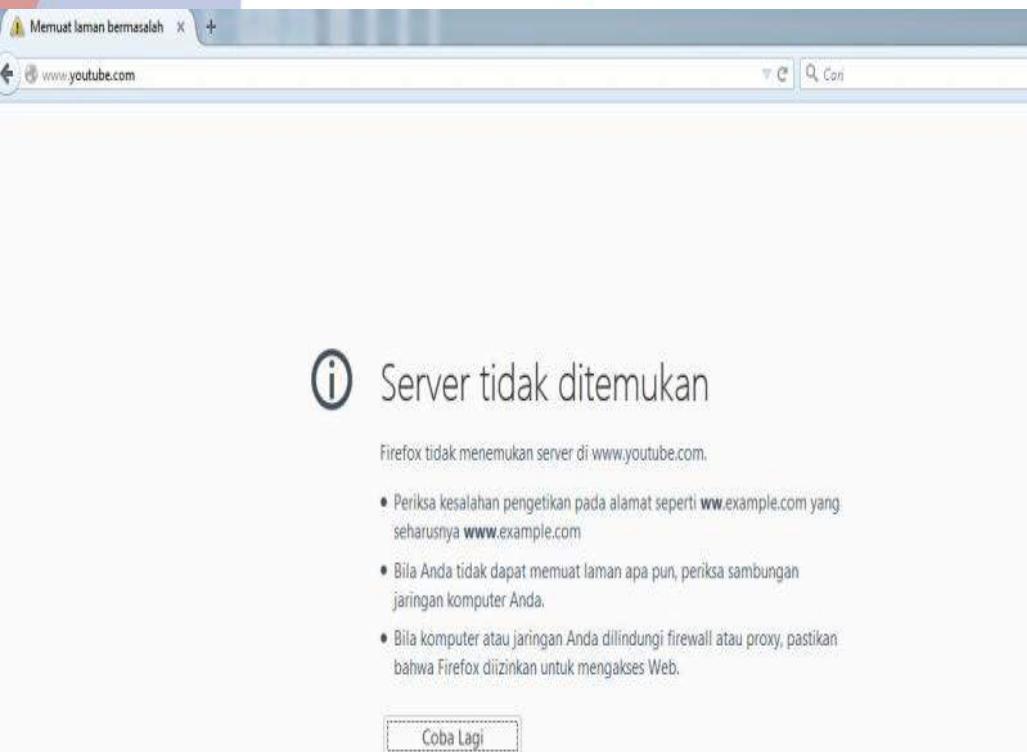


- ✓ Reboot mikrotik router board, dengan cara klik menu System > Reboot

Pengujian hasil konfigurasi *Firewall Jaringan*

Pengujian dilaksanakan setelah dilakukan konfigurasi firewall. Pengujian dilakukan dengan menggunakan laptop atau HP android.

- ✓ Pengaturan IP address pada laptop/android adalah obtain karena telah dilakukan pengaturan DHCP pada either 3 (hospot)
- ✓ Sambungkan Laptop atau Android melalui hosspot Wifi Lab 2 TKJ.
- ✓ Buka browser Chrome ketikkan youtube pada url link nya. Kemudian jalankan



- ✓ Ketika PC melakukan akses ke <http://www.youtube.com> pada web browser, yang hasilnya situs tersebut sudah tidak bisa diakses lagi



Terima
Kasih

LAMPIRAN

LEMBAR PENILAIAN PENGETAHUAN PESERTA DIDIK

Sekolah : SMK Binawiyata Karangmalang Sragen
Kelas/Semester : XII TKJ / 5
Mata pelajaran : Administrasi Infrastruktur Jaringan (AIJ)
Materi Pembelajaran : *firewall* jaringan

Kompetensi Dasar dan Indikator Pencapaian Kompetensi:

Kompetensi Dasar	Indikator Pencapaian Kompetensi
3.10 Mengevaluasi <i>firewall</i> jaringan	3.10.1 Menentukan prasyarat <i>firewall</i> jaringan
4.10 Mengkonfigurasi <i>firewall</i> jaringan	3.10.2 Menganalisis jenis <i>firewall</i> jaringan
	3.10.3 Memilih prosedur dan teknik konfigurasi <i>firewall</i> jaringan
	4.10.1 Melakukan konfigurasi <i>firewall</i> jaringan
	4.10.2 Menguji hasil konfigurasi <i>firewall</i> jaringan

Tujuan Pembelajaran :

Melalui kegiatan pembelajaran dengan pendekatan saintifik, TPACK dan model pembelajaran Discovery Learning , *Project Based Learning*:

1. Peserta didik (A) dapat **mengidentifikasi** tentang *firewall* jaringan (B) setelah membaca Power point dan melihat literatur *firewall* jaringan (C) dengan tepat dan mandiri (D)
2. Peserta didik (A) mampu **menganalisis** jenis *firewall* jaringan (B) melalui tayangan video *firewall* jaringan (C) dengan tepat dan mandiri (D)
3. Peserta didik (A) mampu **memilih** prosedur dan teknik konfigurasi *firewall* jaringan (B) melalui tayangan video *firewall* jaringan (C) dengan percaya diri dan tanggung jawab (D)
4. Peserta didik (A) mampu **mengkonfigurasi** *firewall* jaringan (B) setelah berdiskusi tentang prosedur dan teknik konfigurasi *firewall* jaringan (C) dengan percaya diri dan tanggung jawab (D)
5. Peserta didik (A) mampu **menguji** hasil konfigurasi *firewall* jaringan (B) setelah berdiskusi tentang menguji hasil konfigurasi *firewall* jaringan (C) dengan percaya diri dan tanggung jawab (D)

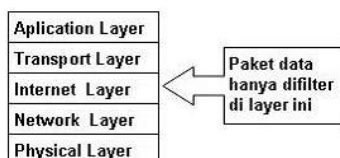
A= Audience; B= Behaviour; C= Condition; D= Degree

Kisi-Kisi Penulisan Soal Evaluasi

No.	Kompetensi Dasar	Indikator Pencapaian Kompetensi	Lingkup Materi	Materi	Indikator Soal	Nomor Soal	Level	Bentuk Soal
1	3.10 Mengevaluasi <i>firewall</i> jaringan	3.10.1 Menentukan prasyarat <i>firewall</i> jaringan 3.10.2 Menganalisis jenis <i>firewall</i> jaringan 3.10.3 Memilih cara konfigurasi <i>firewall</i> jaringan	<i>firewall</i> jaringan	<i>firewall</i> jaringan	Menentukan prasyarat <i>firewall</i> jaringan Menganalisis jenis <i>firewall</i> jaringan Memilih cara konfigurasi <i>firewall</i> jaringan	1 2 3 4 5 6 7	C4 C4 C4 C4 C4 C4 C4	Pilihan Ganda Pilihan Ganda Pilihan Ganda Pilihan Ganda Pilihan Ganda Pilihan Ganda Pilihan Ganda
2	4.10 Mengkonfigurasi <i>firewall</i> jaringan	4.10.1 Melakukan konfigurasi <i>firewall</i> jaringan 4.10.2 Menguji hasil konfigurasi <i>firewall</i> jaringan		Konfigurasi <i>firewall</i> jaringan Pengujian Hasil konfigurasi <i>firewall</i> jaringan	Melakukan konfigurasi <i>firewall</i> jaringan Menguji hasil konfigurasi <i>firewall</i> jaringan	8 9 10	C4 C4 C4	Pilihan Ganda Pilihan Ganda Pilihan Ganda

Soal Evaluasi

1. Firewall didefinisikan sebagai suatu cara atau mekanisme yang diterapkan baik terhadap hardware, software ataupun system itu sendiri dengan tujuan untuk melindungi, baik dengan menyaring, membatasi atau bahkan menolak suatu atau semua hubungan/kegiatan suatu segmen pada jaringan pribadi dengan jaringan luar yang bukan merupakan ruang lingkungannya. Pembatasan terhadap suatu segmen pada jaringan antara lain....
 - A. Terhadap web Youtube
 - B. Terhadap web detik
 - C. Terhadap web yahoo
 - D. Terhadap web linux
 - E. Semua jawaban benar
2. Perhatikan proses yang terjadi pada firewall berikut :
 1. Modifikasi header paket,
 2. Translasi alamat jaringan, dan
 3. Filter paketProses yang digunakan untuk memodifikasi kualitas layanan bit paket TCP sebelum mengalami proses routing terdapat pada nomor...
 - A. Nomor 1.
 - B. Nomor 2
 - C. Nomor 3
 - D. Nomor 1 dan 2.
 - E. Nomor 1 dan 3.
3. 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 berkaitan dengan hardware (pengamanan fisik, sumber daya listrik) maupun yang berkaitan dengan software (sistem, konfigurasi, sistem akses, dll). Pernyataan yang kurang tepat dibawah ini terletak pada.....
 - A. Gangguan pada sistem dapat terjadi karena faktor ketidaksengajaan
 - B. Gangguan pada sistem dapat terjadi karena faktor disengaja orang lain
 - C. Gangguan pada sistem dapat terjadi karena factor human error
 - D. Gangguan pada sistem dapat terjadi karena factor cuaca
 - E. Gangguan pada sistem dapat terjadi karena factor system yang rusak karena penyusunan orang tidak dikenal.
4. Perhatikan gambar berikut ini:

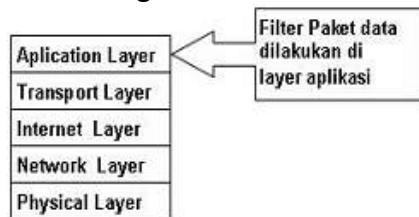


Filterisasi paket ini hanya terbatas pada sumber paket, tujuan paket, dan atribut-atribut dari paket tersebut, misalnya paket tersebut bertujuan ke server kita yang menggunakan alamat IP 202.51.226.35 dengan port 80. Port 80 adalah atribut yang dimiliki oleh paket tersebut. Ini adalah jenis firewall...

- A. *Packet Filtering Gateway*
- B. *Packet Filtering data*

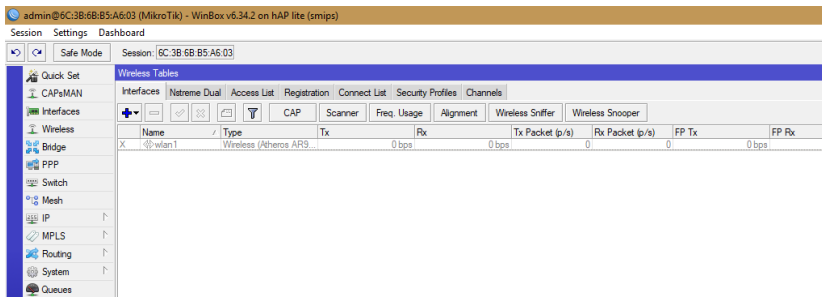
- C. *Application Layer Gateway*
- D. *Circuit Level Gateway*
- E. *Statefull Multilayer Inspection Firewall*

5. Perhatikan gambar berikut ini:



Mekanisme lainnya yang terjadi adalah paket tersebut tidak akan secara langsung sampai ke server tujuan, akan tetapi hanya sampai firewall saja. Selebihnya firewall ini akan membuka koneksi baru ke server tujuan setelah paket tersebut diperiksa berdasarkan aturan yang berlaku. Bila kita melihat dari sisi layer TCP/IP, firewall jenis ini akan melakukan filterisasi pada layer aplikasi (Application Layer. Ini adalah jenis firewall...

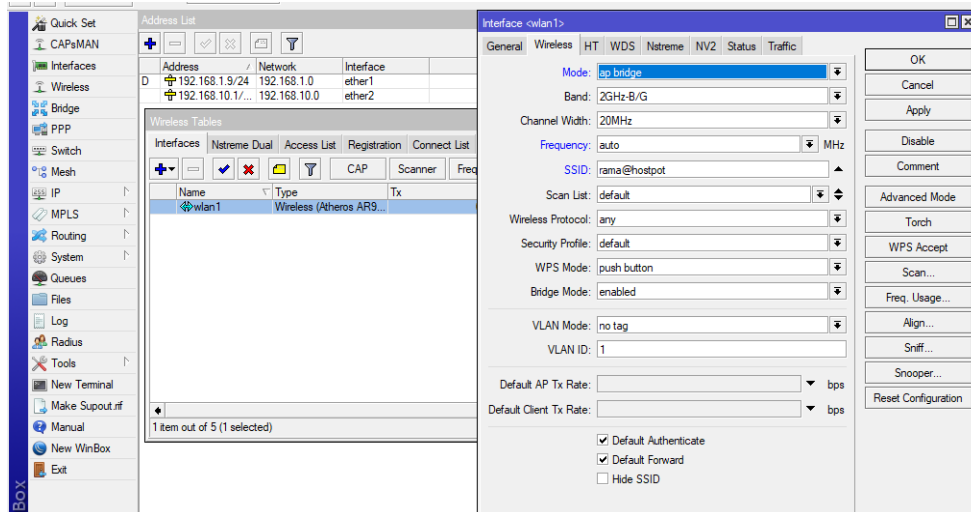
- A. *Packet Filtering Gateway*
 - B. *Packet Filtering data*
 - C. *Application Layer Gateway*
 - D. *Circuit Level Gateway*
 - E. *Statefull Multilayer Inspection Firewall*
6. Model firewall ini bekerja pada bagian Lapisan Transport model referensi TCP/IP. Firewall ini akan melakukan pengawasan terhadap awal hubungan TCP yang biasa disebut sebagai TCP Handshaking, yaitu proses untuk menentukan apakah sesi hubungan tersebut diperbolehkan atau tidak. Bentuknya hampir sama dengan Application Layer Gateway, hanya saja bagian yang difilter terdapat ada lapisan yang berbeda, yaitu berada pada layer Transport. Ini adalah jenis firewall adalah...
- A. *Packet Filtering Gateway*
 - B. *Packet Filtering data*
 - C. *Application Layer Gateway*
 - D. *Circuit Level Gateway*
 - E. *Statefull Multilayer Inspection Firewall*
7. Sistem yang menampilkan informasi statistik akan besar atau banyaknya paket-paket yang melewati sebuah router. Maka dengan fitur ini kita bisa melakukan monitoring terhadap sebuah jaringan dan memungkinkan bagi kita untuk mengidentifikasi berbagai macam masalah yang terjadi di dalamnya. Selain itu, dengan memanfaatkan fitur ini kita dapat melakukan analisa dan meningkatkan performa dari router. Dari daftar diatas, Sistem monitor pada firewall yang diterapkan pada system jaringan ini adalah..
- A. *Simple Packet Flow*
 - B. *Connection Tracking.*
 - C. *Connection tracking*
 - D. *Implikasi Connection State.*
 - E. *Traffic Flow*
8. Pada menu Wireless, klik centang atau enable berwarna biru seperti yang nampak pada gambar berikut:



Langkah konfigurasi ini adalah

- A. Konfigurasi Wireless untuk membuat profil password
- B. Konfigurasi Wireless untuk membuat nama wifi
- C. Konfigurasi Wireless untuk membuat repeater
- D. Mengaktifkan Wireless untuk menuju ke langkah berikutnya
- E. Mengaktifkan Wireless untuk memberikan IP address

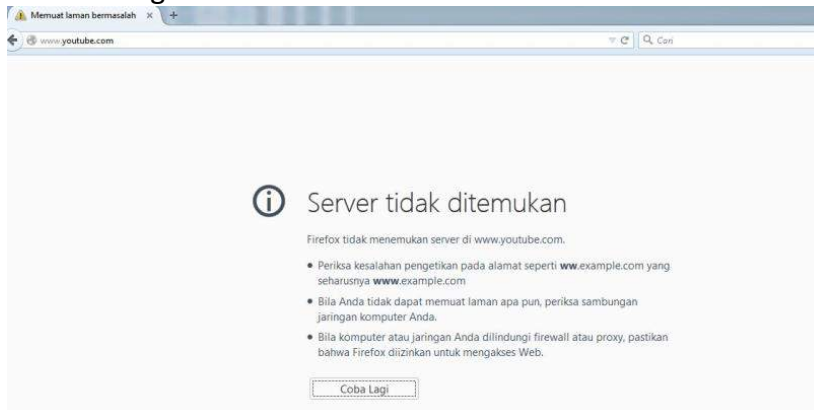
9. Perhatikan gambar berikut



Langkah konfigurasi ini adalah..

- A. Konfigurasi Wireless untuk membuat profil password
- B. Konfigurasi Wireless untuk membuat nama wifi
- C. Konfigurasi Wireless untuk membuat repeater
- D. Mengaktifkan Wireless untuk menuju ke langkah berikutnya
- E. Mengaktifkan Wireless untuk memberikan IP address.

10. Perhatikan gambar berikut



Hasil pengujian konfigurasi firewall untuk membatasi PC Client terhadap web youtube, jika kita ping www.youtube dari CMD client, maka tampilan di cmd adalah...

- A. Reuest Time Out
- B. ReplyTTL
- C. Destination Host Unreashable
- D. General Faillure
- E. Semua salah

Kunci Jawaban Test Formatif

1. E
2. A
3. D
4. A
5. C
6. D
7. E
8. D
9. B
10. C
11. A

Instrumen Penilaian Pengetahuan

No.	Nama Peserta Didik	Nomor Soal										Skor Nilai
		1	2	3	4	5	6	7	8	9	10	
1												
2												
3												
4												
5												
6												

Skor Pengetahuan = jumlah soal benar dikalikan bobot 10.

Keterangan:

Nomor Soal	Bobot
1	10
2	10
3	10
4	10
5	10
6	10
7	10
8	10
9	10
10	10
Jumlah Skor	100

LEMBAR REMIDIAL PESERTA DIDIK

Dengan mengerjakan ulang soal evaluasi

Instrumen Penilaian Remedial

No.	Nama Peserta Didik	Nomor Soal										Skor Nilai
		1	2	3	4	5	6	7	8	9	10	
1												
2												
3												

Skor Pengetahuan = jumlah soal benar dikalikan bobot 10.

Keterangan:

Nomor Soal	Bobot
1	10
2	10
3	10
4	10
5	10
6	10
7	10
8	10
9	10
10	10
Jumlah Skor	100

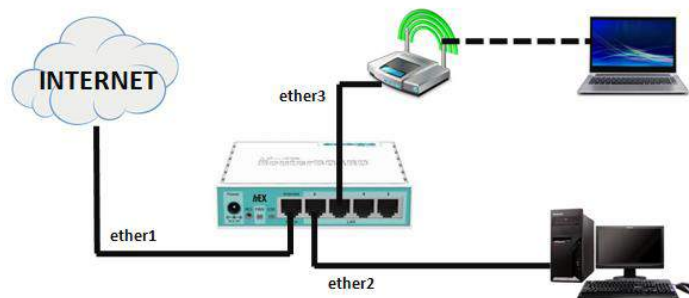
LEMBAR PENGAYAAN PESERTA DIDIK

Studi Kasus :

Membangun Gateway internet, DNS, menggunakan mikrotik routerboard.

Konfigurasi Router :

- IP Internet/ether1 : 192.168.104.2/24
- IP ether2 (LAN) : 192.168.10.0/24
- IP ether3 (AP) : 192.168.20.0/24
- Gateway : 192.168.104.0
- DHCP Server : ether2 (LAN) dan ether3 (AP)
- DNS : 202.57.16.9 – 202.57.16.10
- NAT : MASQUERADE (aktif)



Jenis kegiatan:

1. Menganalisis kebutuhan perangkat jaringan
2. Membangun sebuah internet gateway dengan topologi dan persyaratan seperti uraian persyaratan di atas.

Rubrik Penilaian :

No	Aspek	Penilaian (Skala 100)	Skor yg didapat
1	Tahap persiapan (pemilihan alat dan K3)	Tidak Sesuai (5), Kurang Sesuai (7), Sesuai (8), Sangat Sesuai (10)	
2	Tahap Proses (penyambungan perangkat dan konfigurasinya)	Tidak benar (25), Kurang benar (30), benar(35), Sangat benar (40)	
3	Tahap uji coba hasil konfigurasi	Tidak sesuai (25), Kurang sesuai (30), sesuai (35), Sangat sesuai (40)	
4	Waktu	Tidak tepat (5), Kurang tepat (7), tepat (8), Sangat tepat (10)	
Jumlah (Max. 100)			

Nilai		Paraf Guru
	<p>(.....)* <i>*Tulis nama dan tanda tangan</i></p> <p>(.....)* <i>*Tulis nama dan tanda tangan</i></p> <p>(.....)* <i>*Tulis nama dan tanda tangan</i></p> <p>(.....)* <i>*Tulis nama dan tanda tangan</i></p>	<p><u>Sujarwoko, ST, S.Kom</u></p>

LEMBAR PENILAIAN SIKAP PESERTA DIDIK

Sekolah : SMK Binawiyata Karangmalang Sragen
Kelas/Semester : XII TKJ / 5
Mata pelajaran : Administrasi Infrastruktur Jaringan (AIJ)
Materi Pembelajaran : Gateway Internet

Kompetensi Inti (KI)

1. Menghargai dan menghayati ajaran agama yang dianutnya.
2. Menghargai dan menghayati perilaku jujur, disiplin, tanggung jawab, peduli (toleransi, gotong royong), santun, percaya diri, dalam berinteraksi secara efektif dengan lingkungan sosial dalam jangkauan pergaulan dan keberadaannya.
3. Memahami pengetahuan (faktual, konseptual, dan prosedural) berdasarkan rasa ingin tahunya tentang ilmu pengetahuan, teknologi, seni, budaya terkait fenomena dan kejadian tampak mata.
4. Mencoba, mengolah, dan menyaji dalam ranah konkret (menggunakan, mengurai, merangkai, memodifikasi, dan membuat) dan ranah abstrak (menulis, membaca, menghitung, menggambar, dan mengarang) sesuai dengan yang dipelajari di sekolah dan sumber lain yang sama dalam sudut pandang/teori.

Kompetensi Dasar dan Indikator Pencapaian Kompetensi:

Kompetensi Dasar	Indikator Pencapaian Kompetensi
3.8 Mengevaluasi Gateway Internet	3.8.1 Menentukan prasyarat internet gateway (NAT)
4.8 Mengkonfigurasi Gateway Internet	3.8.2 Menganalisis jenis internet gateway (NAT)
	3.8.3 Memilih prosedur dan teknik konfigurasi internet gateway (NAT)
	4.8.1 Melakukan konfigurasi internet gateway (NAT)
	4.8.2 Menguji hasil konfigurasi internet gateway (NAT)

Tujuan Pembelajaran :

Melalui kegiatan pembelajaran dengan pendekatan saintifik, TPACK dan model pembelajaran Discovery Learning , *Project Based Learning*:

1. Peserta didik (A) dapat **menentukan** prasyarat internet gateway (NAT) (B) setelah membaca Power point dan melihat literatur internet gateway (NAT) (C) dengan tepat dan mandiri (D)
2. Peserta didik (A) mampu **menganalisis** jenis internet gateway (NAT) (B) melalui tayangan video internet gateway (NAT) (C) dengan tepat dan mandiri (D)
3. Peserta didik (A) mampu **memilih** prosedur dan teknik konfigurasi internet gateway (NAT) (B) melalui tayangan video internet gateway (NAT) (C) dengan percaya diri dan tanggung jawab (D)
4. Peserta didik (A) mampu **mengkonfigurasi** internet gateway (NAT) (B) setelah berdiskusi tentang prosedur dan teknik konfigurasi internet gateway (NAT) (C) dengan percaya diri dan tanggung jawab (D)

5. Peserta didik (A) mampu **menguji** hasil konfigurasi internet gateway (NAT) (B) setelah berdiskusi tentang menguji hasil konfigurasi internet gateway (NAT) (C) dengan percaya diri dan tanggung jawab (D)

A= Audience; B= Behaviour; C= Condition; D= Degree

Petunjuk:

Lembaran ini diisi oleh guru untuk menilai sikap spiritual dan sosial siswa. Berilah tanda cek (☑) pada kolom skor sesuai sikap yang ditampilkan oleh siswa, dengan kriteria sebagai berikut:

- SB : Sangat Baik, apabila selalu melakukan sesuai pernyataan.
- B : Baik, apabila sering melakukan sesuai pernyataan dan kadang-kadang tidak melakukan.
- C : Cukup, apabila kadang-kadang melakukan dan sering tidak melakukan
- K : Kurang, apabila tidak pernah melakukan.

Nama Siswa :
 Kelas :
 Tanggal Pengamatan :

No.	Aspek yang Diamati	Kategori			
		SB	B	C	K
1.	Tingkat kedisiplinan kehadiran.				
2.	Ketepatan mengerjakan tugas.				
3.	Keaktifan dan menyelesaikan tugas diskusi kelompok.				
4.	Keaktifan dalam menanggapi presentasi kelompok lain.				
5.	Sikap menyampaikan pendapat di forum diskusi.				
6.	Sikap menghargai pendapat orang lain.				
7.	Sikap tanggung jawab dalam kelompok diskusi.				
8.	Sikap kerja sama dalam menyelesaikan tugas.				
9.	Sikap menyimak penjelasan guru.				
10.	Sikap mengikuti pembelajarans.				
11.	Sikap kemandirian				
Skor Perolehan					
Nilai Sikap (Perolehan Kategori terbanyak: SB,B,C,K)					

LEMBAR KERJA PESERTA DIDIK (LKPD)

Pertemuan 1

Sekolah : SMK Binawiyata Karangmalang Sragen
Kelas/Semester : XII TKJ / 5
Mata pelajaran : Administrasi Infrastruktur Jaringan (AIJ)
Materi Pembelajaran : Firewall Jaringan
Alokasi Waktu : 1 x 15 menit

Nama

Kelompok/Kelas.....

A. KOMPETENSI DASAR & INDIKATOR PENCAPAIAN KOMPETENSI

KOMPETENSI DASAR	INDIKATOR PENCAPAIAN KOMPETENSI
3.10 Mengevaluasi <i>firewall</i> jaringan	3.10.1 Mengidentifikasi tentang <i>firewall</i> jaringan 3.10.2 Menganalisis jenis <i>firewall</i> jaringan 3.10.3 Memilih prosedur dan teknik konfigurasi <i>firewall</i> jaringan

B. TUJUAN PEMBELAJARAN

1. Peserta didik (A) dapat **menentukan** prasyarat *firewall* jaringan (B) setelah membaca Power point dan melihat literatur *firewall* jaringan (C) dengan tepat dan mandiri (D)
2. Peserta didik (A) mampu **menganalisis** jenis *firewall* jaringan (B) melalui tayangan video *firewall* jaringan (C) dengan tepat dan mandiri (D)
3. Peserta didik (A) mampu **memilih** prosedur dan teknik konfigurasi *firewall* jaringan (B) melalui tayangan video *firewall* jaringan (C) dengan percaya diri dan tanggung jawab (D)
A= Audience; B= Behaviour; C= Condition; D= Degree

C. KEGIATAN

1. Tulislah jawaban dari permasalahan yang diberikan pada LKPD ini secara mandiri.
2. Pelajari bahan ajar dan Video Pembelajaran yang sudah dishare pada Google Classroom
Bahan ajar, Link:
<https://docs.google.com/document/d/1V6W8xGscs8VrBsW6eGbbOrrbZAWe-9Xa/edit?usp=sharing&oid=116664950317361593071&rtpof=true&sd=true>

Media Power point: link

https://docs.google.com/presentation/d/1R4TGGxCK_Ff4dCMh9-N9J2sOvIS1eAQW/edit?usp=sharing&oid=116664950317361593071&rtpof=true&sd=true

Video Youtube: Firewall Jaringan (Konsep, Fitur dan jenis), link :

https://www.youtube.com/watch?v=9vzi1O_RuXY

Video Youtube: konfigurasi : Firewall Jaringan, link:

https://www.youtube.com/watch?v=9Va9sLJE_0Q&t=13s

Soal.

1. Jelaskan Prinsip kerja atau konsep serta jenis-jenis Firewall Jaringan dengan baik dan benar.
(nilai maksimal 50Point)

2. Tuliskan prosedur dan teknik konfigurasi dengan baik dan benar sesuai dengan video simulasi yang sudah dipresentasikan oleh guru. (nilai maksimal 50Point)

Jawaban

No 1 Prinsip kerja atau konsep serta jenis-jenis Firewall Jaringan

PENGETA HUAN	
No	Jelaskan Prinsip kerja atau konsep internet gateway (NAT) dengan baik dan benar.
1.	<p>.....</p> <p>.....</p> <p>.....</p> <p>.....</p> <p>.....</p> <p>.....</p> <p>.....</p> <p>.....</p> <p>.....</p> <p>.....</p> <p>.....</p> <p>.....</p> <p>.....</p> <p>.....</p> <p>.....</p> <p>.....</p> <p>.....</p> <p>.....</p> <p>.....</p> <p>.....</p>
	(maksimal point = 40) Nilai =

2. Tulislah prosedur dan teknik konfigurasi internet gateway (NAT)

KETRAMPILAN		
No	Tuliskan prosedur dan teknik konfigurasi internet gateway (NAT)	Nilai
1	(jenis perangkat yang dibutuhkan)	(maksimal point=100)
	

2.	(Teknik konfigurasinya)	(maksimal point=100)
TotalPoint (maksimalpoint=60) =((skor/10)*60%)		Nilai =.....

Nomor	Nilai Essay	Paraf Siswa	Paraf Penguji
1		
2		
Jumlah Total Nilai		

D. Komentar Guru/Feedback

.....

E. Monitoring

Tanggal Pemberian Tugas :

Tanggal Penilaian :

Jumlah Nilai :

Nilai	Nilai	Paraf Guru
	(.....)* *Tulis nama dan tanda tangan	
	(.....)* *Tulis nama dan tanda tangan	
	(.....)* *Tulis nama dan tanda tangan	
	(.....)* *Tulis nama dan tanda tangan	<u>Sujarwoko, ST, S.Kom</u>

LEMBAR KERJA PESERTA DIDIK (LKPD)

Pertemuan 2

Sekolah : SMK Binawiyata Karangmalang Sragen
Kelas/Semester : XII TKJ / 5
Mata pelajaran : Administrasi Infrastruktur Jaringan (AIJ)
Materi Pembelajaran : Konfigurasi *firewall* jaringan
Pengujian hasil konfigurasi *firewall* jaringan
Alokasi Waktu : 1 x 15 menit

Nama :

Kelompok/Kelas:

A. KOMPETENSI DASAR & INDIKATOR PENCAPAIAN KOMPETENSI

KOMPETENSI DASAR	INDIKATOR PENCAPAIAN KOMPETENSI
4.10 Mengkonfigurasi <i>firewall</i> jaringan	4.10.1 Melakukan konfigurasi <i>firewall</i> jaringan 4.10.2 Menguji hasil konfigurasi <i>firewall</i> jaringan

B. TUJUAN PEMBELAJARAN

- Peserta didik (A) mampu **mengkonfigurasi** *firewall* jaringan (B) setelah berdiskusi tentang prosedur dan teknik konfigurasi *firewall* jaringan (C) dengan percaya diri dan tanggung jawab (D)
- Peserta didik (A) mampu **menguji** hasil konfigurasi *firewall* jaringan (B) setelah berdiskusi tentang menguji hasil konfigurasi *firewall* jaringan (C) dengan percaya diri dan tanggung jawab (D)

C. KEGIATAN

- Pelajari bahan ajar dan Video Pembelajaran yang sudah dishare pada Google Classroom
Bahan ajar, Link:
<https://docs.google.com/document/d/1V6W8xGscs8VrBsW6eGbbOrrbZAWe-9Xa/edit?usp=sharing&oid=116664950317361593071&rtpof=true&sd=true>

Media Power point: link

https://docs.google.com/presentation/d/1R4TGGxCK_Ff4dCMh9-N9J2sOvIS1eAQW/edit?usp=sharing&oid=116664950317361593071&rtpof=true&sd=true

Video Youtube: Firewall Jaringan (Konsep, Fitur dan jenis), link :

https://www.youtube.com/watch?v=9vzi1O_RuXY

Video Youtube: konfigurasi Firewall Jaringan, link:

https://www.youtube.com/watch?v=9Va9sLJE_0Q&t=13s

Instruksi kerja

Alat dan Bahan :

1. PC / Laptop
2. Internet
3. Router Board 750
4. Aplikasi Winbox

5. Kabel UTP

Sikap Keselamatan kerja :

1. Berdoa sebelum memulai kegiatan belajar
2. Pakailah seragam praktik saat melakukan kegiatan praktik
3. Bekerja secara mandiri dan penuh tanggung jawab
4. Bacalah dan pahami petunjuk soal / langkah kerja praktik dengan cermat
5. Setelah selesai kembalikan alat dan bahan praktik ke tempat semula
6. Merapikan ruang praktik

Langkah Kerja :

1. Siswa masuk ruangan lab dengan rapi
2. Siswa membaca soal/gambar/instruksi kerja yang telah dipersiapkan oleh guru
3. Siswa menyiapkan alat dan bahan yang diperlukan
4. Siswa melakukan kerja proyek mengkonfigurasi *firewall* jaringan sesuai dengan instruksi yang diberikan.
5. Siswa melakukan uji koneksi, PC client tidak dapat mengakses www.youtube.com, tetapi dapat mengakses situs yang lainnya

Gambar Kerja :



Hasil diskusi siswa tentang langkah-langkah konfigurasi dan pengujian *firewall* jaringan:

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

D. Komentar Guru/Feedback

Nilai		Paraf Guru
	<p>(.....)* <i>*Tulis nama dan tanda tangan</i></p> <p>(.....)* <i>*Tulis nama dan tanda tangan</i></p> <p>(.....)* <i>*Tulis nama dan tanda tangan</i></p> <p>(.....)* <i>*Tulis nama dan tanda tangan</i></p>	<p><u>Sujarwoko, ST, S.Kom</u></p>