Modul Ajar

**SISTEM KEAMANAN JARINGAN**

## Modul 2

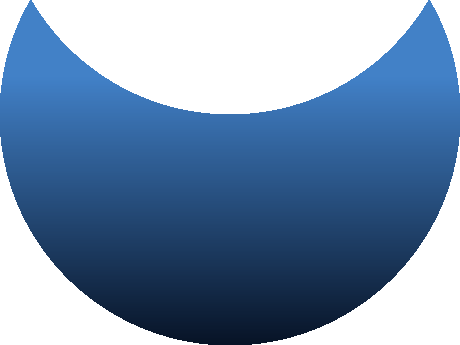
Memahami Firewall dan

Manajemen Proxy

Idiarso, S.Kom

SISTEM INFORMASI

JARINGAN DAN APLIKASI



Kelas XI Semester 2

MODUL AJAR FASE F

# Mod Ajar Kelas XI Sem 2

Berikut adalah revisi dan penulisan ulang sesuai dengan saran yang telah diberikan:

## Informasi Umum

Identitas dan Informasi Umum

|  |  |
| --- | --- |
| **Informasi** | **Detail** |
| **Penyusun** | Idiarso, S.Kom |
| **Nama Sekolah** | SMKN 1 Punggelan |
| **Program Keahlian** | Pengembangan Perangkat Lunak dan Gim |
| **Konsentrasi Keahlian** | Sistem Informasi, Jaringan, dan Aplikasi |
| **Mata Pelajaran** | Sistem Keamanan Jaringan |
| **Elemen** | Keamanan Jaringan dan Deteksi Ancaman |
| **Fase** | F |
| **Lingkup Materi** | Memahami Firewall dan Manajemen Proxy |
| **Kelas / Semester** | XI / Genap |
| **Tahun Pelajaran** | 2023/2024 |
| **Alokasi Waktu** | 54 JP x 45 Menit |
| **Jumlah Pertemuan** | 18 TM x 3 JP |

Kompetensi Awal

#### Kompetensi Awal untuk Pembelajaran Penerapan Firewall dan Proxy

Kompetensi awal bertujuan untuk mengidentifikasi sejauh mana peserta didik sudah memahami konsep dasar yang terkait dengan **Firewall** dan **Proxy** sebelum memulai pembelajaran lebih mendalam. Kompetensi awal ini juga membantu pendidik dalam menilai kesiapan peserta didik dan fokus pada area yang membutuhkan penguatan. Berikut adalah beberapa

**kompetensi awal** yang perlu dikuasai oleh peserta didik:

1. Pengetahuan Dasar Tentang Jaringan dan Keamanan:

**Deskripsi:** Peserta didik harus memiliki pemahaman dasar tentang konsep jaringan komputer dan alasan pentingnya menjaga keamanan jaringan. Mereka harus memahami bagaimana data bergerak di jaringan dan apa saja ancaman yang dapat mengganggu keamanannya.

###### Kompetensi:

Menjelaskan apa itu jaringan komputer.

Mengidentifikasi ancaman umum terhadap keamanan jaringan.

Memahami konsep dasar keamanan jaringan dan peran firewall serta proxy dalam perlindungannya.

1. Pemahaman tentang Firewall:

**Deskripsi:** Peserta didik perlu memahami apa itu firewall, jenis-jenis firewall, dan cara kerja dasar firewall dalam mengamankan jaringan dari ancaman luar.

###### Kompetensi:

Mengidentifikasi dan menjelaskan apa itu firewall.

Menjelaskan berbagai jenis firewall (hardware, software, stateful, stateless).

Memahami fungsi dasar firewall dalam menyaring lalu lintas jaringan berdasarkan aturan yang ditetapkan.

1. Pemahaman tentang Proxy Server:

**Deskripsi:** Sebelum memulai penerapan proxy, peserta didik harus memiliki pemahaman dasar tentang fungsi dan jenis- jenis proxy server.

###### Kompetensi:

Menjelaskan apa itu proxy server dan fungsi utamanya.

Mengidentifikasi perbedaan antara jenis-jenis proxy server (forward, reverse, transparent).

Memahami bagaimana proxy digunakan untuk menyaring dan mengarahkan lalu lintas data di jaringan.

1. Konsep Keamanan Jaringan pada Mikrotik dan Ubuntu:

**Deskripsi:** Peserta didik diharapkan memiliki pemahaman tentang penggunaan Mikrotik dan Ubuntu untuk pengelolaan dan konfigurasi firewall serta proxy server di jaringan.

###### Kompetensi:

Mengetahui cara menggunakan Mikrotik untuk mengonfigurasi firewall dan proxy server.

Memahami penggunaan Ubuntu untuk menginstal dan mengonfigurasi proxy server eksternal (misalnya Squid). Memahami langkah-langkah dasar dalam pengelolaan keamanan jaringan dengan kedua perangkat tersebut.

1. Pengetahuan tentang Kebijakan Keamanan dan Pengelolaan Akses:

**Deskripsi:** Peserta didik harus memahami pentingnya kebijakan keamanan jaringan dan cara mengelola akses pengguna dengan alat keamanan seperti firewall dan proxy.

###### Kompetensi:

Mengidentifikasi kebijakan keamanan yang dapat diterapkan di jaringan.

Memahami cara mengelola akses dan membatasi penggunaan sumber daya jaringan melalui pengaturan firewall dan proxy.

Mengetahui konsep dasar dalam pembuatan kebijakan akses berbasis waktu dan port.

1. Pemahaman tentang Monitoring dan Deteksi Ancaman:

**Deskripsi:** Peserta didik harus memiliki pemahaman tentang bagaimana menggunakan alat monitoring untuk mendeteksi ancaman terhadap keamanan jaringan, serta cara menggunakan firewall dan proxy untuk mitigasi ancaman. **Kompetensi:**

Mengetahui cara memonitor lalu lintas jaringan menggunakan Mikrotik dan Ubuntu. Memahami penggunaan log dan analisis trafik jaringan untuk deteksi ancaman.

Mengetahui cara mengonfigurasi firewall dan proxy untuk mencegah atau memitigasi ancaman yang terdeteksi.

1. Pemahaman tentang Penerapan Kebijakan Akses dan Kontrol Pengguna:

**Deskripsi:** Peserta didik diharapkan dapat memahami cara mengimplementasikan kebijakan akses untuk pengguna jaringan dengan menggunakan firewall dan proxy.

###### Kompetensi:

Menyusun kebijakan akses untuk pengguna dalam jaringan.

Menggunakan proxy dan firewall untuk membatasi akses ke situs web atau layanan tertentu berdasarkan kebijakan. Memahami cara melindungi data sensitif dengan mengonfigurasi aturan di firewall dan proxy.

#### Indikator Kompetensi Awal:

* 1. Peserta didik dapat menjelaskan konsep dasar tentang jaringan komputer dan ancaman terhadap keamanannya.
  2. Peserta didik memahami apa itu firewall dan peranannya dalam melindungi jaringan.
  3. Peserta didik dapat menyebutkan jenis-jenis proxy server dan menjelaskan fungsinya.
  4. Peserta didik tahu cara menggunakan perangkat seperti Mikrotik dan Ubuntu untuk pengelolaan keamanan jaringan.
  5. Peserta didik dapat menjelaskan cara mengelola akses pengguna dan implementasi kebijakan jaringan.
  6. Peserta didik dapat menyebutkan cara-cara mendeteksi dan mengatasi ancaman terhadap jaringan.

#### Metode Penilaian Kompetensi Awal:

###### Tes Diagnostik:

Kuesioner tentang dasar-dasar jaringan dan keamanan, jenis firewall dan proxy server, serta penerapan alat tersebut.

###### Diskusi Kelompok:

Diskusi terbuka untuk membahas konsep firewall, proxy, dan penerapannya dalam konteks jaringan sehari-hari.

###### Tugas Praktik:

Mengonfigurasi firewall dan proxy di Mikrotik atau Ubuntu sesuai dengan skenario yang diberikan untuk menilai pemahaman dasar peserta didik terhadap penggunaan alat tersebut.

Profil Pelajar Pancasila

#### Beriman, Bertakwa kepada Tuhan Yang Maha Esa, dan Berakhlak Mulia

**Deskripsi**: Peserta didik mampu menunjukkan nilai-nilai agama dan etika dalam penggunaan teknologi jaringan. Mereka memahami bahwa keberhasilan dalam mengelola dan mengamankan jaringan harus didasarkan pada prinsip kejujuran, tanggung jawab, dan keberlanjutan. Dalam prakteknya, mereka menerapkan prinsip-prinsip tersebut dalam setiap konfigurasi firewall, proxy, dan kebijakan kontrol akses untuk menjaga keamanan data, serta berkomitmen untuk melindungi hak privasi pengguna jaringan.

###### Indikator:

Memahami dan menerapkan prinsip etika dalam mengelola keamanan jaringan. Berkomitmen pada perlindungan data pribadi dan hak pengguna dalam jaringan.

Menjaga integritas dan kerahasiaan informasi selama melaksanakan praktek di lapangan.

#### Bertanggung Jawab dan Mandiri

**Deskripsi**: Peserta didik memiliki sikap tanggung jawab terhadap pengelolaan dan pengamanan jaringan yang telah

dipelajari, seperti firewall dan proxy, serta mampu bekerja secara mandiri dalam menganalisis dan mengatasi masalah yang muncul di jaringan. Mereka bertanggung jawab untuk melindungi sistem dan informasi jaringan dari ancaman

eksternal maupun internal dengan cara yang efektif dan efisien. Mereka juga berperan aktif dalam memitigasi ancaman seperti serangan DDoS dan port scanning, dan dapat mengonfigurasi firewall serta proxy dengan tepat untuk menjaga keberlanjutan dan keamanan jaringan.

###### Indikator:

Mampu mengidentifikasi dan memitigasi ancaman dalam jaringan secara mandiri. Bertanggung jawab dalam menjaga keamanan dan integritas data jaringan.

Mampu membuat keputusan tepat dalam pengelolaan kebijakan akses dan kontrol pengguna di jaringan.

#### Sarana dan Prasarana

Sarana dan prasarana yang diperlukan untuk mendukung pembelajaran materi **Keamanan Jaringan**, terutama yang berfokus pada pengelolaan **firewall**, **proxy**, serta **deteksi dan mitigasi ancaman** menggunakan perangkat Mikrotik dan Ubuntu.

1. Sarana (Fasilitas Pembelajaran)

##### Fasilitas Kelas

**Ruang Kelas** dengan pencahayaan baik, ventilasi yang

memadai, serta kursi meja yang nyaman untuk diskusi dan praktik.

**Proyektor dan Layar Proyeksi** untuk presentasi materi, tutorial video, dan demonstrasi konfigurasi firewall dan proxy.

**Papan Tulis dan Spidol** untuk menjelaskan konsep-konsep dasar serta menggambarkan topologi jaringan dan pengaturan firewall.

**Sound System** untuk memastikan suara terdengar jelas selama presentasi atau sesi diskusi.

##### Komputer dan Perangkat Lunak

**Komputer atau Laptop** dengan spesifikasi yang cukup untuk menjalankan perangkat lunak pengelolaan jaringan seperti Mikrotik RouterOS, Ubuntu, dan software pengelolaan firewall lainnya.

###### Spesifikasi Minimal:

Prosesor Intel Core i3 atau lebih tinggi RAM 4 GB atau lebih

Penyimpanan SSD 120 GB atau lebih

**Mikrotik RouterOS** untuk konfigurasi firewall dan proxy.

**Ubuntu Server** untuk pengelolaan proxy server (misalnya, Squid Proxy) dan VPN.

**Perangkat Jaringan**: Router, switch, dan kabel jaringan (LAN) untuk mendemonstrasikan pengaturan jaringan dan konektivitas.

##### Akses Internet

**Koneksi Internet Stabil** untuk mengakses tutorial online, perangkat lunak, dan referensi materi keamanan jaringan serta untuk mengunduh pembaruan perangkat lunak dan patch keamanan.

**Wi-Fi atau LAN** untuk menghubungkan perangkat di dalam kelas dan memastikan akses ke jaringan lokal untuk simulasi dan praktik pengelolaan firewall dan proxy.

##### Alat dan Bahan Tambahan

**Virtual Machine (VM)** atau **Lab Simulasi Jaringan** untuk menguji dan mempraktikkan konfigurasi firewall dan proxy tanpa risiko terhadap jaringan utama.

**CCTV (Opsional)** untuk monitoring dan pengawasan pada jaringan selama praktik.

1. Prasarana (Fasilitas Pendukung)

##### Ruang Praktikum

**Lab Komputer** dengan Mikrotik RouterOS, Ubuntu Server, serta perangkat lunak untuk konfigurasi dan pengelolaan jaringan lainnya.

**Koneksi Jaringan** untuk menghubungkan semua perangkat di ruang praktikum dan memastikan akses ke materi serta simulasi pengelolaan firewall dan proxy.

**Server atau Virtual Lab** untuk menguji konfigurasi secara real-time dan melakukan simulasi serangan (seperti DDoS atau port scanning) untuk praktik mitigasi ancaman.

##### Jaringan dan Infrastruktur

**Wi-Fi dan LAN** untuk menghubungkan perangkat di ruang praktikum dan memastikan akses ke materi serta simulasi pengelolaan firewall dan proxy.

**Perangkat Jaringan Mikrotik** untuk simulasi dan konfigurasi firewall.

**Router Mikrotik** untuk konfigurasi firewall dan VPN.

**Switch** untuk menghubungkan perangkat di jaringan lokal dan menguji aliran data.

**Firewall** hardware atau perangkat lunak untuk kebijakan kontrol akses.

##### Perangkat Monitoring dan Pengawasan

**Software Monitoring Jaringan** (Wireshark atau PRTG) untuk membantu peserta didik dalam mengidentifikasi ancaman dan menganalisis lalu lintas jaringan.

**IDS/IPS (Intrusion Detection/Prevention System)** untuk memantau aktivitas mencurigakan dalam jaringan selama ujian praktek atau simulasi ancaman.

##### Sumber Daya Belajar

**Buku dan Modul Pembelajaran** tentang keamanan jaringan, firewall, proxy, dan VPN, baik dalam format cetak maupun digital.

**Tutorial Video** dan **Bahan Ajar Online** untuk mendalami pengelolaan firewall, proxy, dan VPN.

**Referensi Materi Pembelajaran** yang disediakan oleh guru.

##### Ketersediaan Fasilitas Tambahan

**Laboratorium Keamanan Jaringan (Opsional)** untuk ujian praktek dengan perangkat keras dan perangkat lunak jaringan yang lebih canggih.

###### Fasilitas Penunjang Lainnya:

**Kamera untuk Demo Praktek** agar peserta didik bisa mengikuti setiap tahapan dengan jelas.

**Whiteboard Digital atau Smartboard** untuk penjelasan interaktif.

Target Peserta Didik

Pembelajaran **Keamanan Jaringan** ini dirancang untuk tiga kategori peserta didik dengan karakteristik yang berbeda:

* + 1. **Peserta Didik Reguler/Tipikal**: Memiliki kemampuan untuk memahami dan mencerna materi ajar dengan mudah. Pembelajaran dilakukan dengan pendekatan sistematis menggunakan berbagai sumber daya.
    2. **Peserta Didik dengan Kesulitan Belajar**: Memiliki keterbatasan dalam gaya belajar. Pendekatan pembelajaran yang lebih individual dan penggunaan media seperti **video tutorial** dan **audio** disarankan.
    3. **Peserta Didik dengan Pencapaian Tinggi**: Cepat mencerna materi ajar dan mampu menerapkannya dengan sangat baik. Pendekatan berbasis **proyek** dan **tugas-tugas yang memerlukan kreativitas** sangat dianjurkan.

Model Pembelajaran: Keamanan Jaringan

###### Model Pembelajaran yang Digunakan Berdasarkan Modul Keamanan Jaringan

Modul tentang keamanan jaringan dengan fokus pada penerapan **firewall** dan **proxy** ini dapat menggunakan berbagai model pembelajaran yang mendukung tujuan pembelajaran yang ingin dicapai, yaitu **pemahaman mendalam**, **keterampilan teknis**, serta **kemampuan untuk mengidentifikasi dan mengatasi ancaman keamanan jaringan**. Berdasarkan konten dan

pendekatan yang diperlukan dalam pembelajaran ini, model pembelajaran yang cocok adalah **model pembelajaran berbasis masalah (Problem-Based Learning / PBL)** dan **model pembelajaran kooperatif**.

#### Model Pembelajaran Berbasis Masalah (Problem-Based Learning / PBL)

###### Deskripsi Model:

Model **Problem-Based Learning (PBL)** adalah pendekatan pembelajaran yang menekankan pada pemecahan masalah nyata yang relevan dengan dunia nyata. Dalam konteks keamanan jaringan, PBL memungkinkan peserta didik untuk

mempelajari penerapan firewall dan proxy server dengan cara yang kontekstual dan aplikatif. PBL mendorong peserta didik untuk berpikir kritis dan menyelesaikan masalah yang ada, yang dalam hal ini berkaitan dengan bagaimana mengamankan sebuah jaringan menggunakan teknologi firewall dan proxy.

###### Langkah-Langkah Model PBL:

* 1. **Identifikasi Masalah:**

Pendidik memberikan masalah yang relevan, seperti ancaman keamanan yang muncul pada jaringan perusahaan atau rumah, dan mengharuskan peserta didik untuk merancang solusi yang menggunakan firewall dan proxy.

Contoh masalah: “Bagaimana cara mengonfigurasi firewall untuk melindungi jaringan perusahaan dari serangan DDoS dan membatasi akses yang tidak sah menggunakan proxy server?”

###### Pencarian Informasi:

Peserta didik bekerja dalam kelompok untuk mencari informasi tentang firewall, jenis-jenis firewall, cara kerja proxy server, serta cara menerapkan solusi dengan menggunakan perangkat seperti **Mikrotik** dan **Ubuntu**.

Pendidik menyediakan materi pembelajaran yang dapat diakses, seperti video tutorial dan artikel, serta referensi tambahan.

###### Diskusi dan Analisis Solusi:

Dalam kelompok, peserta didik mendiskusikan berbagai alternatif solusi untuk masalah yang diberikan, seperti memilih jenis firewall yang tepat dan menentukan kebijakan proxy yang sesuai.

Diskusi ini memungkinkan mereka untuk mengembangkan keterampilan berpikir kritis dan analitis, serta bekerja sama untuk menghasilkan solusi terbaik.

###### Presentasi dan Penyelesaian Masalah:

Setiap kelompok mempresentasikan solusi yang mereka pilih dan jelaskan cara mereka menerapkan firewall serta proxy dalam skenario jaringan yang relevan.

Pendidik memberikan umpan balik dan memperbaiki solusi yang kurang tepat, serta memberikan penjelasan lebih lanjut jika diperlukan.

###### Refleksi:

Peserta didik diharapkan untuk melakukan refleksi terhadap apa yang telah dipelajari, bagaimana cara mereka memecahkan masalah, dan bagaimana mereka bisa mengembangkan keterampilan tersebut lebih lanjut.

###### Keuntungan Model PBL dalam Pembelajaran Keamanan Jaringan:

Membantu peserta didik mengembangkan keterampilan praktis dalam mengonfigurasi dan mengelola firewall dan proxy. Peserta didik dapat melihat penerapan konsep-konsep tersebut dalam konteks dunia nyata.

Meningkatkan keterampilan pemecahan masalah, berpikir kritis, dan kolaborasi.

#### Model Pembelajaran Kooperatif (Cooperative Learning)

###### Deskripsi Model:

Model **Pembelajaran Kooperatif** melibatkan peserta didik untuk bekerja sama dalam kelompok kecil untuk mencapai tujuan bersama. Model ini sangat sesuai untuk pembelajaran topik seperti penerapan firewall dan proxy server, di mana peserta didik harus saling berkolaborasi untuk menyelesaikan tugas praktikum, diskusi, dan analisis kasus.

###### Langkah-Langkah Model Kooperatif:

* 1. **Pembentukan Kelompok:**

Peserta didik dibagi dalam kelompok kecil (4-5 orang per kelompok), yang bertujuan untuk meningkatkan interaksi dan kolaborasi dalam pemecahan masalah.

Kelompok ini akan bekerja bersama dalam setiap pertemuan untuk menyelesaikan tugas praktikum, analisis, dan diskusi.

###### Pemberian Tugas Berbasis Kelompok:

Setiap kelompok diberikan tugas untuk mengonfigurasi firewall dan proxy pada perangkat tertentu (Mikrotik atau Ubuntu) sesuai dengan skenario yang diberikan.

Kelompok juga diminta untuk membuat kebijakan keamanan jaringan berdasarkan

pemahaman yang mereka dapatkan dari pembelajaran.

###### Diskusi Kelompok:

Dalam setiap kelompok, peserta didik mendiskusikan langkah-langkah konfigurasi, potensi masalah yang mungkin timbul, dan solusi yang sesuai dengan kebutuhan jaringan.

Pendidik memberikan kesempatan bagi setiap kelompok untuk bertanya atau berdiskusi terkait kendala yang mereka hadapi selama konfigurasi.

###### Pemantauan dan Umpan Balik:

Pendidik memantau kemajuan setiap kelompok dan memberikan umpan balik terkait proses yang mereka lakukan. Pendidik memastikan setiap peserta didik dalam kelompok terlibat aktif, serta memberikan bimbingan pada bagian yang memerlukan klarifikasi lebih lanjut.

###### Presentasi Kelompok:

Setiap kelompok mempresentasikan hasil praktikum mereka, termasuk alasan memilih jenis firewall dan proxy yang digunakan, serta cara kebijakan akses diterapkan.

Pendidik dan peserta didik lainnya memberikan tanggapan dan kritik yang membangun terhadap hasil presentasi.

###### Refleksi:

Setelah tugas selesai, peserta didik melakukan refleksi tentang proses kolaborasi yang mereka lakukan, apa yang telah mereka pelajari, dan bagaimana cara mereka meningkatkan kemampuan di masa depan.

###### Keuntungan Model Pembelajaran Kooperatif:

Meningkatkan keterampilan kolaboratif dan komunikasi antar peserta didik.

Memfasilitasi pemahaman yang lebih dalam tentang penerapan firewall dan proxy melalui diskusi dan kerja kelompok. Membantu peserta didik belajar secara aktif melalui pengalaman praktikum yang relevan.

#### Penggunaan Teknologi dalam Pembelajaran:

Untuk mendukung kedua model pembelajaran tersebut, teknologi bisa dimanfaatkan sebagai berikut:

###### Simulasi Praktikum Mikrotik dan Ubuntu:

Menggunakan perangkat virtualisasi atau lab jaringan untuk memungkinkan peserta didik melakukan konfigurasi firewall dan proxy secara langsung.

Menggunakan alat monitoring jaringan untuk membantu peserta didik memahami proses deteksi dan mitigasi ancaman di jaringan.

###### Video Pembelajaran dan Tutorial:

Menggunakan video tutorial untuk memberikan contoh pengaturan firewall dan proxy secara langsung pada Mikrotik dan Ubuntu.

Membantu peserta didik memvisualisasikan konsep-konsep yang mereka pelajari dalam bentuk yang lebih mudah dipahami.

###### Aplikasi Kolaboratif (Google Docs, Google Meet, dsb.):

Memanfaatkan aplikasi seperti Google Docs untuk kolaborasi dalam membuat laporan praktikum. Menggunakan Google Meet atau Zoom untuk diskusi kelompok jarak jauh dan konsultasi dengan pendidik.

Dengan penerapan model pembelajaran **PBL** dan **Kooperatif**, peserta didik akan lebih terlibat dalam proses pembelajaran dan dapat mengembangkan keterampilan praktis dalam mengonfigurasi dan mengelola firewall serta proxy server. Model ini juga menekankan kolaborasi dan pemecahan masalah yang merupakan bagian penting dalam bidang keamanan jaringan.

Berikut adalah format yang telah disesuaikan dengan permintaan Anda:

## Komponen Inti

Komponen inti ini sangat penting untuk merencanakan dan menilai proses pembelajaran secara efektif.

#### Tujuan Pembelajaran

Tujuan pembelajaran merupakan elemen yang sangat penting dalam setiap proses pembelajaran. Tujuan yang jelas akan membantu peserta didik mengetahui apa yang akan mereka pelajari dan capai, serta memberikan arah yang jelas bagi

pendidik dalam merancang kegiatan pembelajaran yang relevan. Dalam konteks penerapan **Firewall** dan **Proxy**, tujuan

pembelajaran harus mencakup pemahaman dan keterampilan praktis untuk mengonfigurasi dan mengelola kedua komponen ini dalam pengamanan jaringan.

###### Contoh Tujuan Pembelajaran:

Peserta didik dapat memahami peran dan fungsi **firewall** dalam menjaga keamanan jaringan.

Peserta didik dapat mengonfigurasi **firewall** dan **proxy server** dengan benar untuk melindungi jaringan.

Peserta didik dapat mengidentifikasi jenis-jenis ancaman jaringan dan menggunakan firewall serta proxy untuk mitigasi ancaman tersebut.

#### Asesmen

Asesmen adalah bagian penting dalam mengevaluasi sejauh mana peserta didik mencapai tujuan pembelajaran. Asesmen harus mencakup berbagai aspek pembelajaran, baik pengetahuan teoritis, keterampilan praktis, maupun sikap. Melalui

asesmen yang tepat, pendidik dapat menilai tidak hanya pemahaman peserta didik, tetapi juga keterampilan mereka dalam mengaplikasikan pengetahuan tersebut dalam konteks dunia nyata.

###### Contoh Asesmen:

**Tes Tertulis:** Tes pilihan ganda untuk mengukur pemahaman konsep dasar tentang **firewall** dan **proxy**.

**Praktikum:** Evaluasi keterampilan peserta didik dalam mengonfigurasi **firewall** pada Mikrotik dan **proxy server** di Ubuntu.

**Penilaian Sikap:** Mengukur sikap peserta didik terhadap keamanan jaringan, termasuk kepatuhan terhadap kebijakan keamanan dan etika dalam penggunaan alat.

#### Pemahaman Bermakna

Pemahaman bermakna memastikan bahwa peserta didik tidak hanya belajar fakta-fakta, tetapi juga dapat mengaitkan materi pembelajaran dengan pengalaman nyata dan konteks praktis di dunia nyata. Penerapan **firewall** dan **proxy** tidak hanya sebatas pada pengetahuan teknis, tetapi juga pada pemahaman tentang bagaimana komponen-komponen ini berperan dalam menjaga keamanan dan efisiensi jaringan.

###### Contoh Pemahaman Bermakna:

**Firewall** tidak hanya dipelajari sebagai pengatur lalu lintas data, tetapi juga dipahami sebagai alat yang melindungi data sensitif di jaringan yang rentan terhadap serangan seperti **DDoS** atau **port scanning**.

**Proxy server** tidak hanya dikenal sebagai alat penyaring konten, tetapi juga sebagai alat yang dapat mengoptimalkan performa jaringan dengan caching dan meningkatkan privasi pengguna.

#### Pertanyaan Pemantik

Pertanyaan pemantik digunakan untuk menggugah rasa ingin tahu peserta didik dan mendorong mereka untuk berpikir lebih mendalam tentang topik yang dipelajari. Pertanyaan yang relevan akan memotivasi peserta didik untuk merenungkan konteks praktis dari teori yang mereka pelajari.

###### Contoh Pertanyaan Pemantik:

Apa yang terjadi pada jaringan kita jika firewall tidak diimplementasikan dengan baik? Bagaimana firewall dapat mencegah serangan DDoS pada jaringan perusahaan?

Apa perbedaan antara **firewall stateless** dan **stateful**, dan bagaimana kedua jenis ini mempengaruhi keamanan jaringan?

Apa yang membedakan **proxy transparan** dengan **proxy biasa**, dan dalam kondisi apa Anda akan memilih menggunakan proxy transparan?

Bagaimana penggunaan **proxy server** dapat membantu meningkatkan kecepatan akses ke situs web yang sering dikunjungi dalam jaringan?

#### Kegiatan Pembelajaran

1. Pertemuan Pertama: Pengantar Firewall Kegiatan Pembelajaran

|  |  |
| --- | --- |
| **Kegiatan**  **Pembelajaran** | **Deskripsi** |
| **Pendahuluan (15 Menit)** | 1. Pendidik mengucapkan salam kepada peserta didik dan memulai kegiatan dengan membaca doa. 2. Pendidik melakukan presensi. 3. Peserta didik diberikan kesempatan untuk menceritakan perasaannya, diikuti dengan tanggapan positif dari siswa lain. 4. Pendidik menyampaikan tujuan pembelajaran dan menyepakatinya dengan siswa. 5. Peserta didik diajak untuk menyepakati keyakinan kelas yang akan dilaksanakan selama pembelajaran. 6. Pendidik memberikan pertanyaan pemantik:    * Apakah kalian sudah tahu apa itu firewall?    * Apa yang terjadi jika suatu jaringan tidak memiliki firewall?    * Bagaimana firewall dapat mencegah akses tidak sah dari luar jaringan?    * Apa perbedaan antara firewall stateful dan stateless? |
| **Kegiatan Inti (135 Menit)** | 1. Peserta didik dikelompokkan menjadi beberapa kelompok heterogen untuk diskusi tentang firewall dan perannya dalam keamanan jaringan. 2. **Stimulus Awal**: Tayangan video tentang pengantar firewall, seperti [Video Pengantar Firewall](https://youtu.be/QlT5fEPhmBI). 3. **Sumber Belajar Interaktif**: Pendidik memberikan referensi tambahan berupa video seperti [Definisi dan Fungsi Firewall](https://youtu.be/pKJmb04T0FQ) dan artikel seperti [Firewall: Fungsi, Jenis, dan Contohnya](https://www.niagahoster.co.id/blog/firewall-adalah/). 4. **Simulasi Praktis**: Kelompok peserta didik melakukan simulasi konfigurasi firewall menggunakan perangkat lunak seperti GNS3 atau Packet Tracer (jika tersedia). 5. **Studi Kasus**: Peserta didik diberikan skenario pelanggaran keamanan jaringan dan diminta mendiskusikan bagaimana firewall dapat mencegahnya. Hasil diskusi disusun sebagai rekomendasi kebijakan firewall. 6. **Role-Play Diskusi**: Dalam kelompok, peserta didik bermain peran sebagai "penyedia jaringan" dan "penyerang" untuk mengeksplorasi bagaimana firewall bekerja dalam melindungi jaringan. 7. **Diskusi Implementasi**: Peserta didik membahas penerapan firewall di jaringan sekolah atau rumah, termasuk contoh kasus nyata. 8. **Presentasi Hasil Diskusi**: Setiap kelompok mempresentasikan hasil diskusinya menggunakan media pilihan seperti PowerPoint atau poster. Kelompok lain memberikan tanggapan, dan kelompok memodifikasi hasil mereka berdasarkan masukan.   **Pengayaan**: Peserta didik dengan kemampuan tinggi diberi tugas mengeksplorasi firewall berbasis cloud seperti AWS Security Group atau Azure Firewall dan membandingkannya dengan firewall tradisional. Mereka juga dapat membuat tutorial video tentang pengaturan dasar firewall untuk  dibagikan. |
| **Kegiatan**  **Penutup (15 Menit)** | 1. Guru meminta peserta didik mengisi refleksi pembelajaran melalui Google Forms atau link yang disediakan. 2. Guru meminta perwakilan peserta didik untuk memberikan refleksi singkat secara langsung. 3. Guru memberikan kesimpulan akhir pembelajaran. 4. Guru menjelaskan materi minggu depan dan memberikan tugas membaca ringan atau video tentang **Jenis-Jenis Ancaman Jaringan** sebagai transisi ke pertemuan berikutnya. 5. Guru menutup pembelajaran dengan doa bersama. |

Refleksi Peserta Didik

|  |  |  |  |
| --- | --- | --- | --- |
| **Pertanyaan Refleksi** | **Baik** | **Cukup** | **Kurang** |
| Apakah kalian sudah mengetahui apa itu firewall? | [ ] | [ ] | [ ] |
| Apakah kalian sudah memahami fungsi firewall dalam menjaga keamanan jaringan? | [ ] | [ ] | [ ] |
| Apakah kalian tahu jenis-jenis firewall yang dapat digunakan? | [ ] | [ ] | [ ] |
| Apakah kalian merasa bisa mengidentifikasi penggunaan firewall dalam kehidupan sehari-hari? | [ ] | [ ] | [ ] |
| Apakah kalian menikmati pelajaran tentang pengantar firewall ini? | [ ] | [ ] | [ ] |

|  |  |  |  |
| --- | --- | --- | --- |
| **Pertanyaan Refleksi** | **Baik** | **Cukup** | **Kurang** |
| Apa yang kalian rasa masih belum jelas mengenai firewall? | [ ] | [ ] | [ ] |

Refleksi Pendidik

|  |  |  |
| --- | --- | --- |
| **No** | **Pertanyaan** | **Jawaban** |
| 1 | Apakah pemilihan media pembelajaran telah mencerminkan tujuan pembelajaran yang akan dicapai? | [ ] |
| 2 | Apakah gaya penyampaian materi mampu ditangkap oleh peserta didik? | [ ] |
| 3 | Apakah keseluruhan pembelajaran dapat memberikan makna pembelajaran yang hendak dicapai? | [ ] |
| 4 | Apakah pemilihan metode pembelajaran sudah efektif untuk menerjemahkan tujuan pembelajaran? | [ ] |
| 5 | Apakah pelaksanaan pelajaran hari ini dapat memberikan semangat kepada peserta didik untuk lebih antusias dalam pembelajaran selanjutnya? | [ ] |

Lampiran

* 1. **Lembar Kerja Peserta Didik**: Terlampir.

###### Pengayaan:

Panduan visual langkah demi langkah untuk peserta didik yang membutuhkan bantuan tambahan. Tugas tambahan eksplorasi firewall berbasis cloud untuk peserta didik dengan kemampuan tinggi.

Diskusi etika: Bahas bagaimana firewall dapat digunakan untuk melacak aktivitas pengguna, serta batasannya dalam melindungi privasi.

###### Media Evaluasi Modern:

Gunakan kuis interaktif melalui **Kahoot!** atau **Google Forms** untuk evaluasi singkat setelah pembelajaran.

###### Glosarium:

**Firewall**: Sistem keamanan jaringan untuk memantau dan mengontrol lalu lintas berdasarkan aturan tertentu.

**Packet Filtering**: Proses memfilter data yang lewat berdasarkan aturan yang telah ditetapkan.

**Stateful Inspection**: Teknik firewall yang melacak status koneksi aktif dan memeriksa apakah paket data sesuai dengan status tersebut.

**Proxy**: Server perantara yang digunakan untuk mengontrol akses ke sumber daya di luar jaringan internal.

### 2 Pertemuan Kedua: Arsitektur dan Desain Firewall\*\*

Kegiatan Pembelajaran

|  |  |
| --- | --- |
| **Kegiatan**  **Pembelajaran** | **Deskripsi** |
| **Pendahuluan (15 Menit)** | 1. Pendidik mengucapkan salam kepada peserta didik dan memulai kegiatan dengan membaca doa. 2. Pendidik melakukan presensi. 3. Pendidik memberikan kesempatan kepada beberapa peserta didik untuk membahas materi pertemuan sebelumnya tentang pengantar firewall dan proxy. 4. Pendidik menyepakati keyakinan kelas bersama peserta didik. 5. Pendidik menyampaikan tujuan pembelajaran. 6. Peserta didik diberikan pertanyaan pemantik:    * Apa yang kalian ketahui tentang arsitektur firewall?    * Apa perbedaan antara firewall berbasis perangkat keras dan perangkat lunak? |
| **Kegiatan Inti (135 Menit)** | 1. Peserta didik dikelompokkan menjadi beberapa kelompok heterogen yang telah dibentuk sebelumnya. |

|  |  |
| --- | --- |
| **Kegiatan**  **Pembelajaran** | **Deskripsi** |
|  | 1. **Stimulus Awal**: Peserta didik diberikan tayangan video tentang arsitektur dan desain firewall,   seperti [Video Arsitektur dan Desain Firewall](https://youtu.be/QlT5fEPhmBI).   1. **Penjelasan Pendidik**: Materi tentang arsitektur firewall, jenis-jenis firewall (hardware vs software), dan cara kerjanya dijelaskan dengan menggunakan referensi tambahan, seperti [Firewall](https://youtu.be/pKJmb04T0FQ)  [Hardware](https://youtu.be/pKJmb04T0FQ) dan [Firewall Software](https://youtu.be/LE8AHJacCFM). 2. **Diskusi Kelompok**: Peserta didik membahas berbagai arsitektur firewall, seperti DMZ, dual- homed firewall, dan screened subnet, serta menentukan kelebihan dan kekurangannya. 3. **Simulasi Praktis**: Peserta didik melakukan simulasi desain arsitektur firewall sederhana menggunakan perangkat lunak seperti GNS3, Cisco Packet Tracer, atau alat simulasi lain. 4. **Studi Kasus**: Setiap kelompok diberi kasus penerapan firewall di organisasi atau perusahaan, diminta untuk merancang desain firewall yang cocok, dan menjelaskan pilihan mereka. 5. **Role-Play Diskusi**: Dalam kelompok, peserta didik bermain peran sebagai "penyedia jaringan" yang mendesain firewall dan "klien" yang memiliki kebutuhan keamanan spesifik, untuk mengeksplorasi kebutuhan desain firewall yang berbeda. 6. **Pengayaan**: Peserta didik dengan kemampuan tinggi diminta untuk mengeksplorasi arsitektur firewall berbasis cloud seperti AWS Security Group dan Azure Firewall, serta membandingkannya dengan firewall tradisional.   **Presentasi Hasil Diskusi**: Setiap kelompok mempresentasikan hasil diskusi menggunakan media seperti PowerPoint, poster, atau video pendek. Kelompok lain memberikan tanggapan.  10. **Perbaikan dan Pengumpulan**: Kelompok memperbaiki presentasi berdasarkan masukan, lalu mengumpulkannya untuk penilaian. |
| **Kegiatan Penutup (15 Menit)** | 1. Guru meminta siswa untuk mengisi refleksi pembelajaran melalui Google Forms atau link lain yang telah disediakan. 2. Guru meminta perwakilan peserta didik memberikan refleksi pembelajaran hari ini. 3. Guru memberikan kesimpulan akhir tentang materi arsitektur firewall. 4. Guru menjelaskan materi pertemuan berikutnya tentang "Jenis Ancaman Jaringan dan Cara Mitigasinya." 5. Guru dan peserta didik menutup pembelajaran dengan doa bersama. |

Refleksi Peserta Didik

|  |  |  |  |
| --- | --- | --- | --- |
| **Pertanyaan Refleksi** | **Baik** | **Cukup** | **Kurang** |
| Apakah kalian sudah mengetahui jenis-jenis arsitektur firewall? | [ ] | [ ] | [ ] |
| Apakah kalian sudah memahami perbedaan antara firewall berbasis perangkat keras dan perangkat lunak? | [ ] | [ ] | [ ] |
| Apakah kalian bisa menyebutkan contoh penerapan firewall dalam kehidupan sehari-hari? | [ ] | [ ] | [ ] |
| Apakah kalian merasa lebih paham tentang desain dan arsitektur firewall setelah pertemuan ini? | [ ] | [ ] | [ ] |
| Apa yang masih kurang jelas mengenai desain firewall? | [ ] | [ ] | [ ] |

Refleksi Pendidik

|  |  |  |
| --- | --- | --- |
| **No** | **Pertanyaan** | **Jawaban** |
| 1 | Apakah pemilihan media pembelajaran telah mencerminkan tujuan pembelajaran yang akan dicapai? | [ ] |
| 2 | Apakah gaya penyampaian materi mampu ditangkap oleh peserta didik? | [ ] |
| 3 | Apakah keseluruhan pembelajaran dapat memberikan makna pembelajaran yang hendak dicapai? | [ ] |
| 4 | Apakah pemilihan metode pembelajaran sudah efektif untuk menerjemahkan tujuan pembelajaran? | [ ] |
| 5 | Apakah pelaksanaan pelajaran hari ini dapat memberikan semangat kepada peserta didik untuk lebih antusias dalam pembelajaran selanjutnya? | [ ] |

Lampiran

1. **Lembar Kerja Peserta Didik**: Terlampir.

###### Pengayaan:

Panduan visual langkah demi langkah untuk membantu peserta didik memahami konsep arsitektur firewall.

Tugas tambahan untuk mengeksplorasi arsitektur firewall berbasis cloud untuk peserta didik dengan kemampuan tinggi.

Diskusi tentang kelebihan dan kekurangan firewall hardware vs software dalam skenario nyata.

###### Bahan Bacaan Pendidik dan Peserta Didik:

Artikel: [Firewall: Fungsi, Jenis, dan Contohnya](https://www.niagahoster.co.id/blog/firewall-adalah/).

Buku Elektronik: "Networking Essentials" oleh Cisco Press. Video: [Arsitektur dan Desain Firewall](https://youtu.be/QlT5fEPhmBI).

###### Glosarium:

**Firewall Berbasis Perangkat Keras**: Perangkat fisik yang digunakan untuk memfilter dan mengontrol lalu lintas jaringan.

**Firewall Berbasis Perangkat Lunak**: Aplikasi yang berjalan pada sistem operasi untuk mengontrol lalu lintas data. **DMZ (Demilitarized Zone)**: Zona jaringan yang digunakan untuk menempatkan sumber daya publik yang dilindungi oleh dua firewall.

**Proxy Firewall**: Firewall yang bekerja sebagai perantara untuk memeriksa dan menyaring lalu lintas data.

#### Pertemuan Ketiga: Packet Filtering dengan Mikrotik

Kegiatan Pembelajaran

|  |  |
| --- | --- |
| **Kegiatan**  **Pembelajaran** | **Deskripsi** |
| **Pendahuluan (15 Menit)** | 1. Pendidik mengucapkan salam kepada peserta didik dan memulai kegiatan dengan membaca doa. 2. Pendidik melakukan presensi. 3. Peserta didik diberi kesempatan untuk membahas materi pertemuan sebelumnya tentang arsitektur dan desain firewall. 4. Pendidik menyepakati keyakinan kelas bersama peserta didik. 5. Pendidik menyampaikan tujuan pembelajaran. 6. Peserta didik diberikan pertanyaan pemantik:    * Apa itu packet filtering?    * Mengapa packet filtering penting dalam keamanan jaringan?    * Apa yang akan terjadi jika tidak ada filter paket di jaringan kita? |
| **Kegiatan Inti (135 Menit)** | 1. **Kelompok Diskusi**: Peserta didik dikelompokkan sesuai pembagian sebelumnya untuk berdiskusi. 2. **Stimulus Awal**: Pendidik menayangkan video pendek tentang konsep packet filtering dan penerapannya di Mikrotik, seperti [Video Packet Filtering](https://youtu.be/QlT5fEPhmBI). 3. **Penjelasan Pendidik**: Materi tentang konsep packet filtering, pentingnya filter paket, dan penerapannya di Mikrotik dijelaskan menggunakan contoh kasus. 4. **Referensi Interaktif**: Pendidik memberikan video tambahan, seperti [Packet Filtering di Mikrotik](https://youtu.be/LE8AHJacCFM), dan artikel untuk mendukung pemahaman lebih lanjut. 5. **Simulasi Praktis**: Peserta didik mempraktikkan konfigurasi dasar packet filtering menggunakan perangkat Mikrotik atau simulasi melalui VirtualBox dan GNS3. 6. **Studi Kasus**: Kelompok diberikan skenario ancaman jaringan, seperti serangan port scanning, dan diminta merancang filter paket untuk mengatasinya. 7. **Diskusi Implementasi**: Peserta didik membahas penerapan packet filtering di jaringan rumah atau sekolah, termasuk tantangan yang mungkin dihadapi. 8. **Presentasi Hasil Diskusi**: Kelompok menyusun presentasi tentang konfigurasi packet filtering yang telah dilakukan dan manfaatnya, menggunakan media seperti PowerPoint atau video tutorial pendek.   **Feedback**: Kelompok lain memberikan tanggapan, dan hasil diskusi diperbaiki berdasarkan masukan.  10. **Pengayaan**: Peserta didik dengan kemampuan tinggi diberikan tantangan untuk mengeksplorasi advanced packet filtering, seperti penerapan NAT atau konfigurasi rule chain pada |

|  |  |
| --- | --- |
| **Kegiatan**  **Pembelajaran** | **Deskripsi** |
|  | Mikrotik.  11. Kelompok mengumpulkan hasil akhir untuk dinilai. |
| **Kegiatan Penutup (15 Menit)** | 1. Guru meminta siswa untuk mengisi refleksi pembelajaran melalui Google Forms atau tautan lain yang disediakan. 2. Guru meminta perwakilan peserta didik memberikan refleksi singkat secara langsung. 3. Guru memberikan kesimpulan akhir pembelajaran. 4. Guru menjelaskan materi pertemuan berikutnya tentang **Deteksi Ancaman dan Teknik Mitigasinya**. 5. Guru dan peserta didik menutup pembelajaran dengan doa bersama. |

Refleksi Peserta Didik

|  |  |  |  |
| --- | --- | --- | --- |
| **Pertanyaan Refleksi** | **Baik** | **Cukup** | **Kurang** |
| Apakah kalian sudah memahami konsep dasar packet filtering? | [ ] | [ ] | [ ] |
| Apakah kalian sudah memahami cara konfigurasi packet filtering di Mikrotik? | [ ] | [ ] | [ ] |
| Apakah kalian bisa menyebutkan manfaat dari penggunaan packet filtering dalam pengamanan jaringan? | [ ] | [ ] | [ ] |
| Apakah kalian merasa lebih paham tentang penggunaan Mikrotik untuk packet filtering setelah pertemuan ini? | [ ] | [ ] | [ ] |
| Apa yang masih kurang jelas mengenai konfigurasi packet filtering dengan Mikrotik? | [ ] | [ ] | [ ] |

Refleksi Pendidik

|  |  |  |
| --- | --- | --- |
| **No** | **Pertanyaan** | **Jawaban** |
| 1 | Apakah pemilihan media pembelajaran telah mencerminkan tujuan pembelajaran yang akan dicapai? | [ ] |
| 2 | Apakah gaya penyampaian materi mampu ditangkap oleh peserta didik? | [ ] |
| 3 | Apakah keseluruhan pembelajaran dapat memberikan makna pembelajaran yang hendak dicapai? | [ ] |
| 4 | Apakah pemilihan metode pembelajaran sudah efektif untuk menerjemahkan tujuan pembelajaran? | [ ] |
| 5 | Apakah pelaksanaan pelajaran hari ini dapat memberikan semangat kepada peserta didik untuk lebih antusias dalam pembelajaran selanjutnya? | [ ] |

Lampiran

* 1. **Lembar Kerja Peserta Didik**: Terlampir.

###### Pengayaan:

Untuk peserta didik yang kesulitan, diberikan panduan visual langkah demi langkah untuk konfigurasi dasar packet filtering di Mikrotik.

Tugas tambahan berupa eksplorasi rule chain dan advanced filtering untuk peserta didik dengan kemampuan tinggi. Diskusi tentang bagaimana filter paket dapat diterapkan dalam skala besar dan kecil.

###### Bahan Bacaan dan Referensi:

Artikel: [Konfigurasi Mikrotik untuk Packet Filtering](https://www.academia.edu/16832625/Pemrograman_web_statis_dan_dinamis).

Video: [Pengertian dan Konfigurasi Packet Filtering di Mikrotik](https://youtu.be/LE8AHJacCFM).

Glosarium

1. **Packet Filtering**: Teknik untuk memfilter paket data yang masuk atau keluar jaringan berdasarkan aturan tertentu.
2. **Mikrotik**: Perangkat jaringan yang digunakan untuk mengelola konfigurasi jaringan, termasuk firewall dan packet filtering.
3. **Rule Chain**: Sekumpulan aturan yang digunakan dalam packet filtering untuk mengontrol lalu lintas data.
4. **NAT (Network Address Translation)**: Teknik untuk memetakan alamat IP lokal ke alamat IP publik untuk keamanan dan penghematan IP.

#### Pertemuan Keempat: Konfigurasi dan Pengelolaan Firewall

Kegiatan Pembelajaran

|  |  |
| --- | --- |
| **Kegiatan**  **Pembelajaran** | **Deskripsi** |
| **Pendahuluan (15 Menit)** | 1. Pendidik mengucapkan salam kepada peserta didik dan memulai kegiatan dengan membaca doa. 2. Pendidik melakukan presensi. 3. Peserta didik diberi kesempatan untuk membahas materi pertemuan sebelumnya tentang packet filtering dan penerapannya menggunakan Mikrotik. 4. Pendidik menyepakati keyakinan kelas bersama peserta didik. 5. Pendidik menyampaikan tujuan pembelajaran. 6. Peserta didik diberikan pertanyaan pemantik:    * Apa saja aturan dasar yang perlu diterapkan dalam konfigurasi firewall?    * Mengapa pengelolaan firewall sangat penting dalam sebuah jaringan? |
| **Kegiatan Inti (135 Menit)** | 1. **Kelompok Diskusi**: Peserta didik dikelompokkan sesuai pembagian sebelumnya untuk berdiskusi. 2. **Stimulus Awal**: Pendidik menayangkan video tentang konfigurasi dan pengelolaan firewall, seperti [Konfigurasi Firewall Mikrotik](https://youtu.be/5gZkJtKz0N8). 3. **Penjelasan Pendidik**: Materi tentang konfigurasi firewall pada Mikrotik dijelaskan dengan menyoroti aturan dasar, kebijakan akses, pembuatan aturan firewall, dan pengelolaan log. 4. **Referensi Interaktif**: Pendidik memberikan video tambahan, seperti [Panduan Konfigurasi](https://www.academia.edu/16832625/Pemrograman_web_statis_dan_dinamis)  [Mikrotik](https://www.academia.edu/16832625/Pemrograman_web_statis_dan_dinamis), untuk mendukung pemahaman lebih lanjut. 5. **Simulasi Praktis**: Peserta didik mempraktikkan konfigurasi firewall pada Mikrotik, termasuk membuat aturan dasar untuk memfilter lalu lintas data dan mengelola log firewall. 6. **Studi Kasus**: Kelompok diberikan skenario ancaman jaringan, seperti akses tidak sah, dan diminta membuat aturan firewall yang sesuai untuk menangani ancaman tersebut. 7. **Diskusi Implementasi**: Peserta didik membahas penerapan aturan firewall dalam lingkungan jaringan kecil, seperti sekolah atau rumah. 8. **Presentasi Hasil Diskusi**: Kelompok menyusun presentasi tentang langkah konfigurasi firewall dan manfaatnya, menggunakan media seperti PowerPoint atau video tutorial pendek.   **Feedback**: Kelompok lain memberikan tanggapan, dan hasil diskusi diperbaiki berdasarkan masukan.   1. **Pengayaan**: Peserta didik dengan kemampuan tinggi diberikan tantangan untuk mengeksplorasi advanced firewall configuration, seperti NAT (Network Address Translation) atau advanced logging pada Mikrotik. 2. Kelompok mengumpulkan hasil akhir untuk dinilai. |
| **Kegiatan Penutup (15 Menit)** | 1. Guru meminta siswa untuk mengisi refleksi pembelajaran melalui Google Forms atau tautan lain yang telah disediakan. 2. Guru meminta perwakilan peserta didik memberikan refleksi singkat secara langsung. 3. Guru memberikan kesimpulan akhir pembelajaran. 4. Guru menjelaskan materi pertemuan berikutnya tentang **Deteksi Ancaman dan Teknik Mitigasinya**. 5. Guru dan peserta didik menutup pembelajaran dengan doa bersama. |

Refleksi Peserta Didik

|  |  |  |  |
| --- | --- | --- | --- |
| **Pertanyaan Refleksi** | **Baik** | **Cukup** | **Kurang** |
| Apakah kalian sudah memahami langkah-langkah dalam konfigurasi firewall di Mikrotik? | [ ] | [ ] | [ ] |
| Apakah kalian sudah memahami pentingnya pengelolaan log firewall dalam menjaga keamanan jaringan? | [ ] | [ ] | [ ] |
| Apakah kalian merasa lebih paham tentang bagaimana mengelola dan mengonfigurasi firewall setelah pertemuan ini? | [ ] | [ ] | [ ] |
| Apakah kalian dapat menyebutkan aturan dasar dalam pengelolaan firewall? | [ ] | [ ] | [ ] |
| Apa yang masih kurang jelas mengenai pengelolaan dan konfigurasi firewall di Mikrotik? | [ ] | [ ] | [ ] |

Refleksi Pendidik

|  |  |  |
| --- | --- | --- |
| **No** | **Pertanyaan** | **Jawaban** |
| 1 | Apakah pemilihan media pembelajaran telah mencerminkan tujuan pembelajaran yang akan dicapai? | [ ] |
| 2 | Apakah gaya penyampaian materi mampu ditangkap oleh peserta didik? | [ ] |
| 3 | Apakah keseluruhan pembelajaran dapat memberikan makna pembelajaran yang hendak dicapai? | [ ] |
| 4 | Apakah pemilihan metode pembelajaran sudah efektif untuk menerjemahkan tujuan pembelajaran? | [ ] |
| 5 | Apakah pelaksanaan pelajaran hari ini dapat memberikan semangat kepada peserta didik untuk lebih antusias dalam pembelajaran selanjutnya? | [ ] |

Lampiran

* 1. **Lembar Kerja Peserta Didik**: Terlampir.

###### Pengayaan:

Untuk peserta didik yang kesulitan, diberikan panduan visual langkah demi langkah untuk konfigurasi firewall di Mikrotik.

Tugas tambahan berupa eksplorasi advanced firewall configuration untuk peserta didik dengan kemampuan tinggi. Diskusi tentang bagaimana log firewall digunakan untuk memantau dan mengaudit jaringan.

###### Bahan Bacaan dan Referensi:

Artikel: [Konfigurasi Mikrotik untuk Firewall](https://www.academia.edu/16832625/Pemrograman_web_statis_dan_dinamis).

Video: [Pengertian dan Konfigurasi Firewall di Mikrotik](https://youtu.be/5gZkJtKz0N8).

Glosarium

1. **Firewall Configuration**: Proses pengaturan aturan untuk memfilter lalu lintas data yang masuk dan keluar dari jaringan menggunakan perangkat firewall.
2. **Log Firewall**: Catatan aktivitas yang dilakukan oleh firewall yang berfungsi untuk memantau dan mengaudit lalu lintas jaringan.
3. **Mikrotik**: Perangkat keras jaringan yang sering digunakan untuk mengatur konfigurasi keamanan jaringan seperti firewall, routing, dan manajemen bandwidth.
4. **NAT (Network Address Translation)**: Teknik untuk memetakan alamat IP lokal ke alamat IP publik untuk keamanan dan penghematan IP.

#### Pertemuan Kelima: Monitor dan Log Aktivitas Firewall

Kegiatan Pembelajaran

|  |  |
| --- | --- |
| **Kegiatan**  **Pembelajaran** | **Deskripsi** |
| **Pendahuluan (15 Menit)** | 1. Pendidik mengucapkan salam kepada peserta didik dan memulai kegiatan dengan membaca doa. 2. Pendidik melakukan presensi. 3. Peserta didik diberi kesempatan untuk membahas materi pertemuan sebelumnya tentang konfigurasi dan pengelolaan firewall. 4. Pendidik menyepakati keyakinan kelas bersama peserta didik. 5. Pendidik menyampaikan tujuan pembelajaran. 6. Peserta didik diberikan pertanyaan pemantik:    * Mengapa monitoring dan logging penting dalam pengelolaan firewall?    * Apa yang dimaksud dengan log firewall, dan bagaimana cara membacanya? |
| **Kegiatan Inti (135 Menit)** | 1. **Kelompok Diskusi**: Peserta didik dikelompokkan sesuai pembagian sebelumnya untuk berdiskusi. 2. **Stimulus Awal**: Pendidik menayangkan video tentang monitoring dan logging aktivitas firewall, seperti [Monitoring Firewall Mikrotik](https://youtu.be/LE8AHJacCFM). 3. **Penjelasan Pendidik**: Materi tentang fungsi monitoring, cara membaca log firewall, dan penggunaannya untuk mendeteksi ancaman dijelaskan dengan contoh kasus. 4. **Referensi Interaktif**: Pendidik memberikan video tambahan dan artikel, seperti [Panduan](https://www.academia.edu/16832625/Pemrograman_web_statis_dan_dinamis)  [Monitoring Mikrotik](https://www.academia.edu/16832625/Pemrograman_web_statis_dan_dinamis), untuk mendukung pemahaman lebih lanjut. 5. **Simulasi Praktis**: Peserta didik mempraktikkan langkah-langkah untuk mengaktifkan fitur logging dan monitoring di Mikrotik, serta menganalisis log yang dihasilkan. 6. **Studi Kasus**: Kelompok diberikan skenario ancaman jaringan, seperti deteksi port scanning atau percobaan akses tidak sah, dan diminta membaca log untuk mengidentifikasi ancaman tersebut. 7. **Diskusi Implementasi**: Peserta didik membahas pentingnya log firewall dalam audit keamanan jaringan, serta tantangan yang mungkin muncul saat membaca log pada jaringan besar. 8. **Presentasi Hasil Diskusi**: Kelompok menyusun presentasi tentang langkah-langkah monitoring dan analisis log firewall menggunakan media seperti PowerPoint, poster, atau video tutorial.   **Feedback**: Kelompok lain memberikan tanggapan, dan hasil diskusi diperbaiki berdasarkan masukan.   1. **Pengayaan**: Peserta didik dengan kemampuan tinggi diberi tugas tambahan untuk mengeksplorasi advanced logging features, seperti analisis berbasis script pada Mikrotik atau penggunaan tools monitoring eksternal. 2. Kelompok mengumpulkan hasil akhir untuk dinilai. |
| **Kegiatan Penutup (15 Menit)** | 1. Guru meminta siswa untuk mengisi refleksi pembelajaran melalui Google Forms atau tautan lain yang telah disediakan. 2. Guru meminta perwakilan peserta didik memberikan refleksi singkat secara langsung. 3. Guru memberikan kesimpulan akhir pembelajaran. 4. Guru menjelaskan materi pertemuan berikutnya tentang **Deteksi Ancaman Jaringan dan Teknik Mitigasi**. 5. Guru dan peserta didik menutup pembelajaran dengan doa bersama. |

Refleksi Peserta Didik

|  |  |  |  |
| --- | --- | --- | --- |
| **Pertanyaan Refleksi** | **Baik** | **Cukup** | **Kurang** |
| Apakah kalian sudah memahami cara memonitor aktivitas firewall? | [ ] | [ ] | [ ] |
| Apakah kalian sudah memahami bagaimana membaca log aktivitas firewall? | [ ] | [ ] | [ ] |
| Apakah kalian merasa lebih paham tentang pentingnya monitoring dan logging dalam pengelolaan firewall setelah pertemuan ini? | [ ] | [ ] | [ ] |
| Apakah kalian dapat menyebutkan langkah-langkah dasar dalam memonitor aktivitas firewall? | [ ] | [ ] | [ ] |
| Apa yang masih kurang jelas mengenai cara mengaktifkan dan membaca log firewall di Mikrotik? | [ ] | [ ] | [ ] |

Refleksi Pendidik

|  |  |  |
| --- | --- | --- |
| **No** | **Pertanyaan** | **Jawaban** |
| 1 | Apakah pemilihan media pembelajaran telah mencerminkan tujuan pembelajaran yang akan dicapai? | [ ] |
| 2 | Apakah gaya penyampaian materi mampu ditangkap oleh peserta didik? | [ ] |
| 3 | Apakah keseluruhan pembelajaran dapat memberikan makna pembelajaran yang hendak dicapai? | [ ] |
| 4 | Apakah pemilihan metode pembelajaran sudah efektif untuk menerjemahkan tujuan pembelajaran? | [ ] |
| 5 | Apakah pelaksanaan pelajaran hari ini dapat memberikan semangat kepada peserta didik untuk lebih antusias dalam pembelajaran selanjutnya? | [ ] |

Lampiran

* 1. **Lembar Kerja Peserta Didik**: Terlampir.

###### Pengayaan:

Panduan visual langkah demi langkah untuk membantu peserta didik yang kesulitan memahami fitur logging dan monitoring.

Tugas tambahan untuk mengeksplorasi fitur advanced logging bagi peserta didik dengan kemampuan tinggi.

Diskusi tentang bagaimana monitoring firewall dapat diintegrasikan dengan tools analitik eksternal, seperti Splunk atau Zabbix.

###### Bahan Bacaan dan Referensi:

Artikel: [Panduan Mikrotik dan Log Firewall](https://www.academia.edu/16832625/Pemrograman_web_statis_dan_dinamis).

Video: [Monitor dan Log Aktivitas Firewall di Mikrotik](https://youtu.be/LE8AHJacCFM).

Glosarium

1. **Firewall Monitoring**: Proses untuk memantau aktivitas yang terjadi di jaringan dan mengevaluasi apakah data yang lewat sesuai dengan aturan yang telah ditentukan.
2. **Log Firewall**: Catatan tentang aktivitas yang dilakukan oleh firewall, seperti lalu lintas yang diblokir atau diperbolehkan.
3. **Mikrotik**: Perangkat keras dan perangkat lunak yang digunakan untuk memonitor, mengonfigurasi, dan mengelola jaringan komputer, termasuk firewall dan log-nya.
4. **Packet Logging**: Fitur pada firewall yang merekam informasi tentang paket data yang diproses, termasuk waktu, sumber, tujuan, dan tindakan yang diambil.

#### Pertemuan Keenam: Implementasi Firewall dalam Jaringan

Kegiatan Pembelajaran

|  |  |
| --- | --- |
| **Kegiatan**  **Pembelajaran** | **Deskripsi** |
| **Pendahuluan (15 Menit)** | 1. Pendidik mengucapkan salam kepada peserta didik dan memulai kegiatan dengan membaca doa. 2. Pendidik melakukan presensi. 3. Peserta didik diberi kesempatan untuk membahas materi pertemuan sebelumnya tentang monitoring dan log aktivitas firewall. 4. Pendidik menyepakati keyakinan kelas bersama peserta didik. 5. Pendidik menyampaikan tujuan pembelajaran. 6. Peserta didik diberikan pertanyaan pemantik:    * Mengapa implementasi firewall dalam jaringan sangat penting?    * Apa saja yang perlu diperhatikan saat mengimplementasikan firewall dalam jaringan besar dan kecil? |

|  |  |
| --- | --- |
| **Kegiatan**  **Pembelajaran** | **Deskripsi** |
| **Kegiatan Inti (135 Menit)** | 1. **Kelompok Diskusi**: Peserta didik dikelompokkan sesuai pembagian sebelumnya untuk berdiskusi. 2. **Stimulus Awal**: Pendidik menayangkan video tentang implementasi firewall dalam jaringan menggunakan Mikrotik, seperti [Implementasi Firewall Mikrotik](https://youtu.be/LE8AHJacCFM). 3. **Penjelasan Pendidik**: Materi tentang penerapan firewall dijelaskan dengan menyoroti perbedaan kebutuhan firewall pada jaringan kecil (rumah) dan besar (perusahaan). 4. **Referensi Interaktif**: Pendidik memberikan video tambahan dan artikel, seperti [Panduan](https://www.academia.edu/16832625/Pemrograman_web_statis_dan_dinamis)  [Mikrotik untuk Implementasi Firewall](https://www.academia.edu/16832625/Pemrograman_web_statis_dan_dinamis), untuk mendukung pemahaman lebih lanjut. 5. **Simulasi Praktis**: Peserta didik mempraktikkan penerapan firewall pada skenario jaringan rumah dan kantor kecil menggunakan Mikrotik, termasuk pengaturan rule chain dasar untuk memfilter lalu lintas data. 6. **Studi Kasus**: Kelompok diberikan skenario jaringan besar dengan beberapa cabang dan   diminta untuk merancang penerapan firewall yang sesuai, serta mengidentifikasi potensi tantangan dalam implementasi tersebut.   1. **Diskusi Implementasi**: Peserta didik membahas langkah-langkah dasar penerapan firewall pada berbagai jenis jaringan, termasuk pentingnya scalability dan maintenance. 2. **Presentasi Hasil Diskusi**: Kelompok menyusun presentasi tentang langkah-langkah   implementasi firewall dan tantangan yang mungkin dihadapi, menggunakan media seperti PowerPoint, video tutorial, atau infografis.  **Feedback**: Kelompok lain memberikan tanggapan, dan hasil diskusi diperbaiki berdasarkan masukan.   1. **Pengayaan**: Peserta didik dengan kemampuan tinggi diberikan tantangan tambahan untuk mengeksplorasi fitur-fitur canggih pada firewall Mikrotik, seperti implementasi NAT dan VPN untuk keamanan jaringan. 2. Kelompok mengumpulkan hasil akhir untuk dinilai. |
| **Kegiatan Penutup (15 Menit)** | 1. Guru meminta siswa untuk mengisi refleksi pembelajaran melalui Google Forms atau tautan lain yang telah disediakan. 2. Guru meminta perwakilan peserta didik memberikan refleksi singkat secara langsung. 3. Guru memberikan kesimpulan akhir pembelajaran. 4. Guru menjelaskan materi pertemuan berikutnya tentang **Ancaman Jaringan dan Strategi Pencegahannya**. 5. Guru dan peserta didik menutup pembelajaran dengan doa bersama. |

Refleksi Peserta Didik

|  |  |  |  |
| --- | --- | --- | --- |
| **Pertanyaan Refleksi** | **Baik** | **Cukup** | **Kurang** |
| Apakah kalian sudah memahami bagaimana cara mengimplementasikan firewall dalam jaringan? | [ ] | [ ] | [ ] |
| Apakah kalian sudah mengetahui tantangan yang dihadapi dalam implementasi firewall pada jaringan besar? | [ ] | [ ] | [ ] |
| Apakah kalian merasa lebih paham tentang penerapan firewall dalam jaringan setelah pertemuan ini? | [ ] | [ ] | [ ] |
| Apakah kalian dapat menyebutkan langkah-langkah dasar dalam implementasi firewall di jaringan rumah atau kantor kecil? | [ ] | [ ] | [ ] |
| Apa yang masih kurang jelas mengenai implementasi firewall dalam jaringan besar dan kecil? | [ ] | [ ] | [ ] |

Refleksi Pendidik

|  |  |  |
| --- | --- | --- |
| **No** | **Pertanyaan** | **Jawaban** |
| 1 | Apakah pemilihan media pembelajaran telah mencerminkan tujuan pembelajaran yang akan dicapai? | [ ] |
| 2 | Apakah gaya penyampaian materi mampu ditangkap oleh peserta didik? | [ ] |

|  |  |  |
| --- | --- | --- |
| **No** | **Pertanyaan** | **Jawaban** |
| 3 | Apakah keseluruhan pembelajaran dapat memberikan makna pembelajaran yang hendak dicapai? | [ ] |
| 4 | Apakah pemilihan metode pembelajaran sudah efektif untuk menerjemahkan tujuan pembelajaran? | [ ] |
| 5 | Apakah pelaksanaan pelajaran hari ini dapat memberikan semangat kepada peserta didik untuk lebih antusias dalam pembelajaran selanjutnya? | [ ] |

Lampiran

* 1. **Lembar Kerja Peserta Didik**: Terlampir.

###### Pengayaan:

Panduan visual langkah demi langkah untuk membantu peserta didik memahami penerapan firewall di jaringan rumah dan kantor kecil.

Tugas tambahan untuk mengeksplorasi advanced firewall configuration seperti NAT dan VPN bagi peserta didik dengan kemampuan tinggi.

Diskusi tentang scalability firewall untuk jaringan besar.

###### Bahan Bacaan dan Referensi:

Artikel: [Panduan Mikrotik untuk Implementasi Firewall](https://www.academia.edu/16832625/Pemrograman_web_statis_dan_dinamis). Video: [Implementasi Firewall pada Jaringan Mikrotik](https://youtu.be/LE8AHJacCFM).

Glosarium

1. **Firewall Implementation**: Proses penerapan firewall pada jaringan untuk memantau dan mengontrol lalu lintas data yang masuk dan keluar, sesuai dengan aturan yang telah ditentukan.
2. **Jaringan Rumah**: Jaringan komputer dengan skala kecil yang biasanya digunakan di rumah, melibatkan beberapa perangkat komputer, ponsel, dan perangkat lain yang terhubung ke internet.
3. **Jaringan Perusahaan**: Jaringan komputer yang lebih besar yang digunakan oleh organisasi atau perusahaan untuk menghubungkan berbagai perangkat dan menyediakan layanan jaringan untuk berbagai keperluan bisnis.
4. **Scalability**: Kemampuan suatu sistem untuk menangani peningkatan lalu lintas atau perangkat yang terhubung tanpa penurunan kinerja.

#### Pertemuan Ketujuh: Tantangan dan Tren Terbaru dalam Firewall

Kegiatan Pembelajaran

|  |  |
| --- | --- |
| **Kegiatan**  **Pembelajaran** | **Deskripsi** |
| **Pendahuluan (15 Menit)** | 1. Pendidik mengucapkan salam kepada peserta didik dan memulai kegiatan dengan membaca doa. 2. Pendidik melakukan presensi. 3. Peserta didik diberi kesempatan untuk membahas materi pertemuan sebelumnya tentang implementasi firewall dalam jaringan. 4. Pendidik menyepakati keyakinan kelas bersama peserta didik. 5. Pendidik menyampaikan tujuan pembelajaran. 6. Peserta didik diberikan pertanyaan pemantik:    * Apa tantangan terbesar dalam mengelola firewall saat ini?    * Apa saja tren terbaru dalam teknologi firewall yang perlu diperhatikan? |
| **Kegiatan Inti (135 Menit)** | 1. **Kelompok Diskusi**: Peserta didik dikelompokkan sesuai pembagian sebelumnya untuk berdiskusi. 2. **Stimulus Awal**: Pendidik menayangkan video tentang tantangan dan tren terbaru dalam firewall, seperti [Next-Generation Firewall dan Keamanan Jaringan](https://youtu.be/LE8AHJacCFM). 3. **Penjelasan Pendidik**: Materi tentang tantangan yang dihadapi dalam pengelolaan firewall, |

|  |  |
| --- | --- |
| **Kegiatan**  **Pembelajaran** | **Deskripsi** |
|  | seperti serangan DDoS, malware, serta pentingnya skalabilitas dan integrasi. Pendidik juga  menjelaskan fitur Next-Generation Firewall (NGFW) dan IDS/IPS.   1. **Referensi Interaktif**: Pendidik memberikan video tambahan dan artikel, seperti [Tren Terbaru](https://www.academia.edu/16832625/Pemrograman_web_statis_dan_dinamis)  [dalam Keamanan Jaringan](https://www.academia.edu/16832625/Pemrograman_web_statis_dan_dinamis), untuk mendukung pemahaman lebih lanjut. 2. **Diskusi Tantangan**: Kelompok membahas tantangan dalam firewall, seperti kebutuhan terhadap real-time monitoring, adaptasi terhadap ancaman canggih, dan optimalisasi sumber daya jaringan. 3. **Diskusi Tren**: Peserta didik juga mendiskusikan tren terbaru dalam firewall, seperti penggunaan AI dalam NGFW, integrasi dengan cloud security, dan kolaborasi dengan solusi keamanan lain. 4. **Simulasi Mini**: Kelompok diminta untuk merancang solusi firewall berdasarkan tantangan yang diberikan, misalnya bagaimana NGFW bisa digunakan untuk menangani malware atau serangan DDoS di jaringan besar. 5. **Presentasi Hasil Diskusi**: Kelompok menyusun presentasi tentang tantangan dan tren terbaru dalam firewall serta solusi yang relevan menggunakan media seperti PowerPoint, infografis, atau video pendek.   **Feedback**: Kelompok lain memberikan tanggapan, dan hasil diskusi diperbaiki berdasarkan masukan.   1. **Pengayaan**: Peserta didik dengan kemampuan tinggi diberikan tugas tambahan untuk mengeksplorasi teknologi firewall berbasis AI atau penggunaan firewall dalam konteks IoT (Internet of Things). 2. Kelompok mengumpulkan hasil akhir untuk dinilai. |
| **Kegiatan Penutup (15 Menit)** | 1. Guru meminta siswa untuk mengisi refleksi pembelajaran melalui Google Forms atau tautan lain yang telah disediakan. 2. Guru meminta perwakilan peserta didik memberikan refleksi singkat secara langsung. 3. Guru memberikan kesimpulan akhir pembelajaran. 4. Guru menjelaskan materi pertemuan berikutnya tentang **Strategi Keamanan Holistik untuk Jaringan Masa Depan**. 5. Guru dan peserta didik menutup pembelajaran dengan doa bersama. |

Refleksi Peserta Didik

|  |  |  |  |
| --- | --- | --- | --- |
| **Pertanyaan Refleksi** | **Baik** | **Cukup** | **Kurang** |
| Apakah kalian sudah memahami tantangan utama dalam pengelolaan firewall saat ini? | [ ] | [ ] | [ ] |
| Apakah kalian sudah mengetahui tren terbaru dalam teknologi firewall? | [ ] | [ ] | [ ] |
| Apakah kalian merasa lebih paham tentang teknologi Next-Generation Firewall (NGFW) setelah pertemuan ini? | [ ] | [ ] | [ ] |
| Apakah kalian dapat menyebutkan beberapa solusi terbaru untuk mengatasi tantangan dalam penggunaan firewall? | [ ] | [ ] | [ ] |
| Apa yang masih kurang jelas mengenai tantangan dan tren terbaru dalam firewall? | [ ] | [ ] | [ ] |

Refleksi Pendidik

|  |  |  |
| --- | --- | --- |
| **No** | **Pertanyaan** | **Jawaban** |
| 1 | Apakah pemilihan media pembelajaran telah mencerminkan tujuan pembelajaran yang akan dicapai? | [ ] |
| 2 | Apakah gaya penyampaian materi mampu ditangkap oleh peserta didik? | [ ] |
| 3 | Apakah keseluruhan pembelajaran dapat memberikan makna pembelajaran yang hendak dicapai? | [ ] |
| 4 | Apakah pemilihan metode pembelajaran sudah efektif untuk menerjemahkan tujuan pembelajaran? | [ ] |
| 5 | Apakah pelaksanaan pelajaran hari ini dapat memberikan semangat kepada peserta didik untuk lebih antusias dalam pembelajaran selanjutnya? | [ ] |

Lampiran

* 1. **Lembar Kerja Peserta Didik**: Terlampir.

###### Pengayaan:

Panduan visual langkah demi langkah tentang fitur Next-Generation Firewall (NGFW).

Tugas tambahan untuk mengeksplorasi firewall berbasis AI atau penggunaannya dalam IoT bagi peserta didik dengan kemampuan tinggi.

Diskusi mendalam tentang integrasi firewall dengan sistem keamanan berbasis cloud.

###### Bahan Bacaan dan Referensi:

Artikel: [Tren Terbaru dalam Keamanan Jaringan](https://www.academia.edu/16832625/Pemrograman_web_statis_dan_dinamis).

Video: [Next-Generation Firewall dan Keamanan Jaringan](https://youtu.be/LE8AHJacCFM).

Glosarium

1. **Next-Generation Firewall (NGFW)**: Firewall generasi terbaru yang memiliki kemampuan mendeteksi dan mencegah ancaman canggih serta mendukung integrasi dengan solusi keamanan lainnya.
2. **Serangan DDoS (Distributed Denial of Service)**: Serangan yang bertujuan untuk melumpuhkan layanan dengan membanjiri jaringan dengan trafik palsu.
3. **AI dalam Firewall**: Penggunaan teknologi kecerdasan buatan untuk mendeteksi pola ancaman dan merespons ancaman secara adaptif.
4. **IoT (Internet of Things)**: Jaringan perangkat yang saling terhubung melalui internet, seperti smart home devices, yang memerlukan perlindungan khusus terhadap ancaman keamanan.

#### Pertemuan Kedelapan: Pengantar Proxy Server

Kegiatan Pembelajaran

|  |  |
| --- | --- |
| **Kegiatan**  **Pembelajaran** | **Deskripsi** |
| **Pendahuluan (15 Menit)** | 1. Pendidik mengucapkan salam kepada peserta didik dan memulai kegiatan dengan membaca doa. 2. Pendidik melakukan presensi. 3. Peserta didik diberi kesempatan untuk membahas materi pertemuan sebelumnya tentang firewall dan tantangan terkini dalam keamanan jaringan. 4. Pendidik menyepakati keyakinan kelas bersama peserta didik. 5. Pendidik menyampaikan tujuan pembelajaran. 6. Peserta didik diberikan pertanyaan pemantik:    * Apa itu proxy server?    * Apa perbedaan antara proxy server dan firewall? |
| **Kegiatan Inti (135 Menit)** | 1. **Kelompok Diskusi**: Peserta didik dikelompokkan sesuai pembagian sebelumnya untuk berdiskusi. 2. **Stimulus Awal**: Pendidik menayangkan video tentang pengertian dan fungsi proxy server, seperti [Pengantar Proxy Server](https://youtu.be/QlT5fEPhmBI). 3. **Penjelasan Pendidik**: Materi tentang proxy server dijelaskan dengan menyoroti fungsinya dalam meningkatkan keamanan, mengatur kontrol akses, dan mempercepat akses internet, serta membahas jenis-jenis proxy seperti forward proxy, reverse proxy, dan transparent proxy. 4. **Referensi Interaktif**: Pendidik memberikan video tambahan dan artikel, seperti [Jenis Proxy](https://youtu.be/LE8AHJacCFM) [Server](https://youtu.be/LE8AHJacCFM) dan [Panduan Proxy Server](https://www.academia.edu/16832625/Pemrograman_web_statis_dan_dinamis), untuk mendukung pemahaman lebih lanjut. 5. **Simulasi Praktis**: Peserta didik mempraktikkan konfigurasi dasar proxy server menggunakan software seperti Squid Proxy atau Mikrotik, mencakup pengaturan kontrol akses dan penyaringan konten. 6. **Diskusi Implementasi**: Kelompok mendiskusikan manfaat proxy server dalam mengamankan jaringan dan tantangan yang mungkin dihadapi saat mengonfigurasinya. 7. **Presentasi Hasil Diskusi**: Kelompok menyusun presentasi tentang pengertian, jenis, dan manfaat proxy server menggunakan media seperti PowerPoint, video pendek, atau infografis. 8. **Feedback**: Kelompok lain memberikan tanggapan, dan hasil diskusi diperbaiki berdasarkan masukan. |

|  |  |
| --- | --- |
| **Kegiatan**  **Pembelajaran** | **Deskripsi** |
|  | **Pengayaan**: Peserta didik dengan kemampuan tinggi diberikan tugas tambahan untuk  mengeksplorasi penerapan proxy dalam jaringan perusahaan atau organisasi besar, seperti konfigurasi caching proxy untuk mengoptimalkan kinerja jaringan.  10. Kelompok mengumpulkan hasil akhir untuk dinilai. |
| **Kegiatan**  **Penutup (15 Menit)** | 1. Guru meminta siswa untuk mengisi refleksi pembelajaran melalui Google Forms atau tautan lain yang telah disediakan. 2. Guru meminta perwakilan peserta didik memberikan refleksi singkat secara langsung. 3. Guru memberikan kesimpulan akhir pembelajaran. 4. Guru menjelaskan materi pertemuan berikutnya tentang **Konfigurasi Proxy Server untuk Keamanan dan Efisiensi Jaringan**. 5. Guru dan peserta didik menutup pembelajaran dengan doa bersama. |

Refleksi Peserta Didik

|  |  |  |  |
| --- | --- | --- | --- |
| **Pertanyaan Refleksi** | **Baik** | **Cukup** | **Kurang** |
| Apakah kalian sudah memahami apa itu proxy server dan bagaimana cara kerjanya? | [ ] | [ ] | [ ] |
| Apakah kalian bisa menyebutkan jenis-jenis proxy server yang ada? | [ ] | [ ] | [ ] |
| Apakah kalian merasa lebih paham tentang penerapan proxy server setelah pertemuan ini? | [ ] | [ ] | [ ] |
| Apakah kalian dapat menjelaskan perbedaan antara proxy server dan firewall? | [ ] | [ ] | [ ] |
| Apa yang masih kurang jelas mengenai konfigurasi dan penerapan proxy server? | [ ] | [ ] | [ ] |

Refleksi Pendidik

|  |  |  |
| --- | --- | --- |
| **No** | **Pertanyaan** | **Jawaban** |
| 1 | Apakah pemilihan media pembelajaran telah mencerminkan tujuan pembelajaran yang akan dicapai? | [ ] |
| 2 | Apakah gaya penyampaian materi mampu ditangkap oleh peserta didik? | [ ] |
| 3 | Apakah keseluruhan pembelajaran dapat memberikan makna pembelajaran yang hendak dicapai? | [ ] |
| 4 | Apakah pemilihan metode pembelajaran sudah efektif untuk menerjemahkan tujuan pembelajaran? | [ ] |
| 5 | Apakah pelaksanaan pelajaran hari ini dapat memberikan semangat kepada peserta didik untuk lebih antusias dalam pembelajaran selanjutnya? | [ ] |

Lampiran

* 1. **Lembar Kerja Peserta Didik**: Terlampir.

###### Pengayaan:

Panduan visual langkah demi langkah tentang konfigurasi dasar proxy server.

Tugas tambahan untuk mengeksplorasi penerapan caching proxy dan keamanan tambahan pada proxy server untuk peserta didik dengan kemampuan tinggi.

Diskusi mendalam tentang peran proxy dalam jaringan modern.

###### Bahan Bacaan dan Referensi:

Artikel: [Panduan Proxy Server](https://www.academia.edu/16832625/Pemrograman_web_statis_dan_dinamis).

Video: [Pengertian dan Jenis Proxy Server](https://youtu.be/LE8AHJacCFM).

Glosarium

1. **Proxy Server**: Server perantara yang bertugas untuk mengontrol dan menyaring lalu lintas data antara pengguna dan server lain di internet. Proxy server dapat digunakan untuk mempercepat akses internet, meningkatkan keamanan, dan membatasi akses ke konten tertentu.
2. **Forward Proxy**: Proxy yang digunakan untuk menghubungkan klien ke server di internet, berfungsi untuk menyaring dan memfilter data yang masuk atau keluar.
3. **Reverse Proxy**: Proxy yang digunakan di sisi server untuk mengelola lalu lintas yang datang dari klien, sering digunakan untuk meningkatkan kinerja dan keamanan server.
4. **Transparent Proxy**: Proxy yang tidak memodifikasi permintaan atau respons antara klien dan server, dan tidak memerlukan konfigurasi klien untuk digunakan.

#### Pertemuan Kesembilan: Proxy Internal dengan Mikrotik

Kegiatan Pembelajaran

|  |  |
| --- | --- |
| **Kegiatan**  **Pembelajaran** | **Deskripsi** |
| **Pendahuluan (15 Menit)** | 1. Pendidik mengucapkan salam kepada peserta didik dan memulai kegiatan dengan membaca doa. 2. Pendidik melakukan presensi. 3. Peserta didik diberi kesempatan untuk membahas materi pertemuan sebelumnya tentang proxy server dan penerapannya. 4. Pendidik menyepakati keyakinan kelas bersama peserta didik. 5. Pendidik menyampaikan tujuan pembelajaran. 6. Peserta didik diberikan pertanyaan pemantik:    * Apa manfaat dari penggunaan proxy server internal?    * Apa saja konfigurasi dasar yang perlu dilakukan untuk mengaktifkan proxy server di Mikrotik? |
| **Kegiatan Inti (135 Menit)** | 1. **Kelompok Diskusi**: Peserta didik dikelompokkan sesuai pembagian sebelumnya untuk berdiskusi. 2. **Stimulus Awal**: Pendidik menayangkan video tentang konfigurasi proxy server internal di Mikrotik, seperti [Konfigurasi Proxy Internal Mikrotik](https://youtu.be/QlT5fEPhmBI). 3. **Penjelasan Pendidik**: Materi tentang konfigurasi proxy server internal dijelaskan dengan menyoroti pengaturan cache, filter konten, dan pengelolaan kebijakan akses pengguna di jaringan. 4. **Referensi Interaktif**: Pendidik memberikan video tambahan dan artikel, seperti [Konfigurasi](https://youtu.be/LE8AHJacCFM)  [Proxy Mikrotik](https://youtu.be/LE8AHJacCFM) dan [Panduan Proxy Server Mikrotik](https://www.academia.edu/16832625/Pemrograman_web_statis_dan_dinamis), untuk mendukung pemahaman lebih lanjut. 5. **Simulasi Praktis**: Peserta didik mempraktikkan langkah-langkah konfigurasi proxy server   internal di Mikrotik, termasuk pengaturan kontrol akses dan caching untuk meningkatkan efisiensi jaringan.   1. **Diskusi Manfaat**: Kelompok mendiskusikan manfaat penggunaan proxy internal untuk meningkatkan keamanan dan efisiensi jaringan serta tantangan yang mungkin dihadapi saat implementasi. 2. **Presentasi Hasil Diskusi**: Kelompok menyusun presentasi tentang langkah-langkah konfigurasi proxy server di Mikrotik serta manfaatnya menggunakan media seperti PowerPoint, video pendek, atau infografis. 3. **Feedback**: Kelompok lain memberikan tanggapan, dan hasil diskusi diperbaiki berdasarkan masukan.   **Pengayaan**: Peserta didik dengan kemampuan tinggi diberikan tugas tambahan untuk mengeksplorasi fitur proxy canggih di Mikrotik, seperti advanced content filtering atau log monitoring.  10. Kelompok mengumpulkan hasil akhir untuk dinilai. |
| **Kegiatan Penutup (15 Menit)** | 1. Guru meminta siswa untuk mengisi refleksi pembelajaran melalui Google Forms atau tautan lain yang telah disediakan. 2. Guru meminta perwakilan peserta didik memberikan refleksi singkat secara langsung. 3. Guru memberikan kesimpulan akhir pembelajaran. 4. Guru menjelaskan materi pertemuan berikutnya tentang **Proxy Eksternal untuk Jaringan Skala Besar**. 5. Guru dan peserta didik menutup pembelajaran dengan doa bersama. |

Refleksi Peserta Didik

|  |  |  |  |
| --- | --- | --- | --- |
| **Pertanyaan Refleksi** | **Baik** | **Cukup** | **Kurang** |
| Apakah kalian sudah memahami cara mengonfigurasi proxy server internal di Mikrotik? | [ ] | [ ] | [ ] |
| Apakah kalian sudah memahami manfaat penggunaan proxy server internal untuk keamanan jaringan? | [ ] | [ ] | [ ] |
| Apakah kalian merasa lebih paham tentang penerapan proxy server internal di Mikrotik setelah pertemuan ini? | [ ] | [ ] | [ ] |
| Apakah kalian dapat menyebutkan langkah-langkah dasar dalam konfigurasi proxy internal di Mikrotik? | [ ] | [ ] | [ ] |
| Apa yang masih kurang jelas mengenai pengelolaan kebijakan akses dan kontrol konten menggunakan proxy server di Mikrotik? | [ ] | [ ] | [ ] |

Refleksi Pendidik

|  |  |  |
| --- | --- | --- |
| **No** | **Pertanyaan** | **Jawaban** |
| 1 | Apakah pemilihan media pembelajaran telah mencerminkan tujuan pembelajaran yang akan dicapai? | [ ] |
| 2 | Apakah gaya penyampaian materi mampu ditangkap oleh peserta didik? | [ ] |
| 3 | Apakah keseluruhan pembelajaran dapat memberikan makna pembelajaran yang hendak dicapai? | [ ] |
| 4 | Apakah pemilihan metode pembelajaran sudah efektif untuk menerjemahkan tujuan pembelajaran? | [ ] |
| 5 | Apakah pelaksanaan pelajaran hari ini dapat memberikan semangat kepada peserta didik untuk lebih antusias dalam pembelajaran selanjutnya? | [ ] |

Lampiran

1. **Lembar Kerja Peserta Didik**: Terlampir.

###### Pengayaan:

Panduan visual langkah demi langkah tentang konfigurasi proxy server internal.

Tugas tambahan untuk mengeksplorasi fitur lanjutan seperti log monitoring dan optimasi caching pada proxy Mikrotik bagi peserta didik dengan kemampuan tinggi.

Diskusi mendalam tentang manfaat caching dan filter konten dalam jaringan lokal.

###### Bahan Bacaan dan Referensi:

Artikel: [Panduan Proxy Server Mikrotik](https://www.academia.edu/16832625/Pemrograman_web_statis_dan_dinamis).

Video: [Konfigurasi Proxy Internal Mikrotik](https://youtu.be/LE8AHJacCFM).

Glosarium

1. **Proxy Internal**: Server perantara yang digunakan di dalam jaringan lokal (internal) untuk mengatur dan memfilter lalu lintas yang keluar dan masuk dari jaringan.
2. **Cache**: Penyimpanan sementara data yang sudah pernah diakses agar dapat diakses lebih cepat pada kunjungan

berikutnya. Pada proxy server, cache digunakan untuk menyimpan data yang sering diminta oleh pengguna jaringan.

1. **Kontrol Akses**: Kebijakan yang diterapkan untuk membatasi atau mengizinkan akses ke sumber daya tertentu dalam jaringan berdasarkan kriteria tertentu.
2. **Mikrotik**: Perangkat dan sistem operasi jaringan yang sering digunakan untuk mengonfigurasi dan mengelola berbagai fungsi jaringan seperti routing, firewall, dan proxy server.

#### Pertemuan Kesepuluh: Proxy Eksternal dengan Ubuntu

Kegiatan Pembelajaran

|  |  |
| --- | --- |
| **Kegiatan**  **Pembelajaran** | **Deskripsi** |
| **Pendahuluan (15 Menit)** | 1. Pendidik mengucapkan salam kepada peserta didik dan memulai kegiatan dengan membaca doa. 2. Pendidik melakukan presensi. 3. Pendidik memberikan kesempatan kepada beberapa peserta didik untuk membahas materi pertemuan sebelumnya tentang proxy internal di Mikrotik. 4. Pendidik bersama dengan peserta didik menyepakati keyakinan kelas yang akan dilaksanakan selama pembelajaran. 5. Pendidik menyampaikan tujuan pembelajaran dan menyepakatinya dengan siswa. 6. Peserta didik diberikan pertanyaan pemantik, seperti:    1. Apa itu proxy eksternal?    2. Apa perbedaan antara proxy internal dan proxy eksternal? |
| **Kegiatan Inti (135 Menit)** | 1. Peserta didik dikelompokkan menjadi beberapa kelompok yang telah dibentuk di pertemuan sebelumnya. 2. Peserta didik diberikan stimulus dalam bentuk tayangan video mengenai cara mengonfigurasi proxy eksternal menggunakan Ubuntu. [Video Proxy Eksternal Ubuntu](https://youtu.be/QlT5fEPhmBI) 3. Pendidik menjelaskan materi tentang proxy eksternal, fungsinya dalam mengamankan dan menyaring akses dari internet ke jaringan internal, serta cara konfigurasi proxy eksternal di Ubuntu menggunakan **Squid Proxy**. 4. Pendidik memberikan referensi video yang menjelaskan cara mengonfigurasi proxy eksternal di Ubuntu:    * [Konfigurasi Proxy Eksternal Ubuntu](https://youtu.be/LE8AHJacCFM)    * Buku Elektronik Penunjang: [Panduan Proxy Eksternal Ubuntu](https://www.academia.edu/16832625/Pemrograman_web_statis_dan_dinamis) 5. Peserta didik melakukan latihan untuk mengonfigurasi proxy eksternal di Ubuntu, mengatur   **Squid Proxy** untuk membatasi dan mengontrol akses ke internet dari jaringan internal.   1. Peserta didik diminta untuk mengidentifikasi manfaat penggunaan proxy eksternal dalam meningkatkan keamanan dan pengendalian akses internet. 2. Peserta didik mendiskusikan cara-cara mengelola kebijakan akses, seperti membatasi website atau layanan tertentu melalui proxy eksternal. 3. Peserta didik menyusun dan merangkum langkah-langkah konfigurasi proxy eksternal serta manfaatnya dalam pengelolaan jaringan.   Masing-masing kelompok mempresentasikan hasil latihan dan diskusi mereka menggunakan media seperti PowerPoint, video tutorial, atau naskah cerita.   1. Pendidik meminta kelompok lain untuk memberikan tanggapan terhadap presentasi kelompok lainnya. 2. Setiap kelompok mencatat masukan dan memperbaiki presentasi mereka. 3. Pendidik meminta kelompok untuk mengumpulkan hasil presentasi yang sudah disempurnakan sesuai media yang dipilih. |
| **Kegiatan Penutup (15 Menit)** | 1. Guru meminta siswa untuk mengisi refleksi pembelajaran melalui link yang disediakan. 2. Guru meminta perwakilan peserta didik memberikan refleksi pembelajaran hari ini. 3. Guru memberikan kesimpulan akhir dan meminta siswa yang sudah paham untuk membantu teman-teman yang masih belum memahami. 4. Guru menjelaskan materi minggu depan dan bahan yang perlu dipersiapkan siswa untuk kelancaran pembelajaran berikutnya. 5. Peserta didik dan pendidik mengakhiri pembelajaran dengan doa. |

Refleksi Peserta Didik

|  |  |  |  |
| --- | --- | --- | --- |
| **Pertanyaan Refleksi** | **Baik** | **Cukup** | **Kurang** |
| Apakah kalian sudah memahami cara mengonfigurasi proxy eksternal di Ubuntu? | [ ] | [ ] | [ ] |
| Apakah kalian sudah memahami manfaat penggunaan proxy eksternal untuk kontrol akses internet? | [ ] | [ ] | [ ] |
| Apakah kalian merasa lebih paham tentang perbedaan antara proxy internal dan proxy eksternal setelah pertemuan ini? | [ ] | [ ] | [ ] |

|  |  |  |  |
| --- | --- | --- | --- |
| **Pertanyaan Refleksi** | **Baik** | **Cukup** | **Kurang** |
| Apakah kalian dapat menyebutkan langkah-langkah dasar dalam konfigurasi proxy eksternal di Ubuntu? | [ ] | [ ] | [ ] |
| Apa yang masih kurang jelas mengenai pengelolaan proxy eksternal dan pengaturan kontrol akses internet di Ubuntu? | [ ] | [ ] | [ ] |

Refleksi Pendidik

|  |  |  |
| --- | --- | --- |
| **No** | **Pertanyaan** | **Jawaban** |
| 1 | Apakah pemilihan media pembelajaran telah mencerminkan tujuan pembelajaran yang akan dicapai? | [ ] |
| 2 | Apakah gaya penyampaian materi mampu ditangkap oleh peserta didik? | [ ] |
| 3 | Apakah keseluruhan pembelajaran dapat memberikan makna pembelajaran yang hendak dicapai? | [ ] |
| 4 | Apakah pemilihan metode pembelajaran sudah efektif untuk menerjemahkan tujuan pembelajaran? | [ ] |
| 5 | Apakah pelaksanaan pelajaran hari ini dapat memberikan semangat kepada peserta didik untuk lebih antusias dalam pembelajaran selanjutnya? | [ ] |

Lampiran

* 1. **Lembar Kerja Peserta Didik**: Terlampir.
  2. **Pengayaan**: Untuk peserta didik yang hasil belajarnya belum mencapai target, pendidik melakukan pengulangan materi dengan pendekatan yang lebih individual dan memberikan tugas tambahan untuk memperbaiki hasil belajar peserta didik bersangkutan.

###### Bahan Bacaan Pendidik dan Peserta Didik:

Video tema "Konfigurasi Proxy Eksternal di Ubuntu": [Proxy Eksternal Ubuntu](https://youtu.be/LE8AHJacCFM). Buku Elektronik Penunjang Belajar: [Panduan Proxy Eksternal Ubuntu](https://www.academia.edu/16832625/Pemrograman_web_statis_dan_dinamis).

Glosarium

1. **Proxy Eksternal**: Server yang terletak di luar jaringan internal dan digunakan untuk mengelola akses antara jaringan

internal dan internet. Proxy eksternal berfungsi untuk menyaring, mempercepat, dan mengamankan lalu lintas data yang menuju ke jaringan internal.

1. **Squid Proxy**: Perangkat lunak open-source yang sering digunakan untuk membangun server proxy eksternal. Squid memungkinkan pengelolaan cache, kontrol akses, dan filtering situs web.
2. **Kontrol Akses Internet**: Pengaturan untuk membatasi atau mengizinkan akses pengguna ke situs web atau layanan tertentu melalui penggunaan proxy server. Pengaturan ini sering digunakan untuk meningkatkan keamanan dan

produktivitas di lingkungan jaringan.

#### Pertemuan Kesebelas: Pengaturan Kebijakan Proxy Server

Kegiatan Pembelajaran

|  |  |
| --- | --- |
| **Kegiatan**  **Pembelajaran** | **Deskripsi** |
| **Pendahuluan (15 Menit)** | 1. Pendidik mengucapkan salam kepada peserta didik dan memulai kegiatan dengan membaca doa. 2. Pendidik melakukan presensi. 3. Pendidik memberikan kesempatan kepada beberapa peserta didik untuk membahas materi pertemuan sebelumnya tentang proxy eksternal dan konfigurasi di Ubuntu. 4. Pendidik bersama dengan peserta didik menyepakati keyakinan kelas yang akan dilaksanakan selama pembelajaran. 5. Pendidik menyampaikan tujuan pembelajaran dan menyepakatinya dengan siswa. 6. Peserta didik diberikan pertanyaan pemantik, seperti: |

|  |  |
| --- | --- |
| **Kegiatan**  **Pembelajaran** | **Deskripsi** |
|  | 1. Apa itu kebijakan proxy server? 2. Mengapa pengaturan kebijakan proxy sangat penting dalam sebuah jaringan? |
| **Kegiatan Inti (135 Menit)** | 1. Peserta didik dikelompokkan menjadi beberapa kelompok yang telah dibentuk di pertemuan sebelumnya. 2. Peserta didik diberikan stimulus dalam bentuk tayangan video mengenai pengaturan kebijakan proxy server di Mikrotik dan Ubuntu. [Video Pengaturan Kebijakan Proxy](https://youtu.be/QlT5fEPhmBI) 3. Pendidik menjelaskan materi tentang pengaturan kebijakan proxy server, termasuk pengelolaan akses, pembatasan situs web, dan kontrol akses di jaringan. 4. Pendidik memberikan referensi video yang menjelaskan cara mengatur kebijakan proxy di Mikrotik dan Ubuntu:    * [Pengaturan Kebijakan Proxy Mikrotik](https://youtu.be/LE8AHJacCFM)    * Buku Elektronik Penunjang: [Panduan Kebijakan Proxy Server](https://www.academia.edu/16832625/Pemrograman_web_statis_dan_dinamis) 5. Peserta didik melakukan latihan untuk mengonfigurasi kebijakan proxy server, termasuk pembatasan akses situs, pengaturan filter konten, dan pengelolaan bandwidth. 6. Peserta didik diminta untuk mendiskusikan berbagai kebijakan yang bisa diterapkan dalam proxy server untuk mengontrol akses ke sumber daya jaringan. 7. Peserta didik menyusun dan merangkum langkah-langkah pengaturan kebijakan proxy server serta manfaatnya untuk keamanan jaringan. 8. Masing-masing kelompok mempresentasikan hasil latihan dan diskusi mereka menggunakan media seperti PowerPoint, video tutorial, atau naskah cerita.   Pendidik meminta kelompok lain untuk memberikan tanggapan terhadap presentasi kelompok lainnya.   1. Setiap kelompok mencatat masukan dan memperbaiki presentasi mereka. 2. Pendidik meminta kelompok untuk mengumpulkan hasil presentasi yang sudah disempurnakan sesuai media yang dipilih. |
| **Kegiatan Penutup (15 Menit)** | 1. Guru meminta siswa untuk mengisi refleksi pembelajaran melalui link yang disediakan. 2. Guru meminta perwakilan peserta didik memberikan refleksi pembelajaran hari ini. 3. Guru memberikan kesimpulan akhir dan meminta siswa yang sudah paham untuk membantu teman-teman yang masih belum memahami. 4. Guru menjelaskan materi minggu depan dan bahan yang perlu dipersiapkan siswa untuk kelancaran pembelajaran berikutnya. 5. Peserta didik dan pendidik mengakhiri pembelajaran dengan doa. |

Refleksi Peserta Didik

|  |  |  |  |
| --- | --- | --- | --- |
| **Pertanyaan Refleksi** | **Baik** | **Cukup** | **Kurang** |
| Apakah kalian sudah memahami bagaimana cara mengonfigurasi kebijakan proxy server? | [ ] | [ ] | [ ] |
| Apakah kalian sudah mengetahui cara membatasi akses situs melalui proxy server? | [ ] | [ ] | [ ] |
| Apakah kalian merasa lebih paham tentang pengaturan kebijakan proxy setelah pertemuan ini? | [ ] | [ ] | [ ] |
| Apakah kalian dapat menjelaskan perbedaan antara proxy server dengan kebijakan yang diterapkan di dalamnya? | [ ] | [ ] | [ ] |
| Apa yang masih kurang jelas mengenai pengelolaan kebijakan dan filter konten menggunakan proxy server? | [ ] | [ ] | [ ] |

Refleksi Pendidik

|  |  |  |
| --- | --- | --- |
| **No** | **Pertanyaan** | **Jawaban** |
| 1 | Apakah pemilihan media pembelajaran telah mencerminkan tujuan pembelajaran yang akan dicapai? | [ ] |
| 2 | Apakah gaya penyampaian materi mampu ditangkap oleh peserta didik? | [ ] |
| 3 | Apakah keseluruhan pembelajaran dapat memberikan makna pembelajaran yang hendak dicapai? | [ ] |
| 4 | Apakah pemilihan metode pembelajaran sudah efektif untuk menerjemahkan tujuan pembelajaran? | [ ] |
| 5 | Apakah pelaksanaan pelajaran hari ini dapat memberikan semangat kepada peserta didik untuk lebih antusias dalam pembelajaran selanjutnya? | [ ] |

Lampiran

1. **Lembar Kerja Peserta Didik**: Terlampir.
2. **Pengayaan**: Untuk peserta didik yang hasil belajarnya belum mencapai target, pendidik melakukan pengulangan materi dengan pendekatan yang lebih individual dan memberikan tugas tambahan untuk memperbaiki hasil belajar peserta didik bersangkutan.

###### Bahan Bacaan Pendidik dan Peserta Didik:

Video tema "Pengaturan Kebijakan Proxy Mikrotik dan Ubuntu": [Pengaturan Proxy Mikrotik](https://youtu.be/LE8AHJacCFM). Buku Elektronik Penunjang Belajar: [Panduan Kebijakan Proxy Server](https://www.academia.edu/16832625/Pemrograman_web_statis_dan_dinamis).

Glosarium

1. **Kebijakan Proxy Server**: Aturan atau pengaturan yang diterapkan pada proxy server untuk mengontrol akses ke internet, menyaring konten, membatasi situs web tertentu, dan mengelola penggunaan bandwidth dalam jaringan.
2. **Filter Konten**: Pengaturan pada proxy server yang memungkinkan untuk membatasi akses ke situs atau konten tertentu yang dianggap tidak sesuai atau tidak diinginkan di dalam jaringan.
3. **Proxy Server**: Server yang bertindak sebagai perantara antara klien dan server lain di internet. Proxy server digunakan untuk meningkatkan kinerja, mengamankan jaringan, dan mengontrol akses ke sumber daya di internet.
4. **Bandwidth Management**: Pengelolaan penggunaan bandwidth di jaringan untuk memastikan distribusi lalu lintas yang efisien dan mencegah kelebihan beban pada saluran jaringan.

### Pertemuan Keduabelas: Monitoring Lalu Lintas Jaringan dengan Mikrotik\*\*

Kegiatan Pembelajaran

|  |  |
| --- | --- |
| **Kegiatan**  **Pembelajaran** | **Deskripsi** |
| **Pendahuluan (15 Menit)** | 1. Pendidik mengucapkan salam kepada peserta didik dan memulai kegiatan dengan membaca doa. 2. Pendidik melakukan presensi. 3. Pendidik memberikan kesempatan kepada beberapa peserta didik untuk membahas materi pertemuan sebelumnya tentang pengaturan kebijakan proxy server. 4. Pendidik bersama dengan peserta didik menyepakati keyakinan kelas yang akan dilaksanakan selama pembelajaran. 5. Pendidik menyampaikan tujuan pembelajaran dan menyepakatinya dengan siswa. 6. Peserta didik diberikan pertanyaan pemantik, seperti:    1. Apa yang dimaksud dengan monitoring lalu lintas jaringan?    2. Mengapa penting untuk memantau lalu lintas jaringan pada perangkat Mikrotik? |
| **Kegiatan Inti (135 Menit)** | 1. Peserta didik dikelompokkan menjadi beberapa kelompok yang telah dibentuk di pertemuan sebelumnya. 2. Peserta didik diberikan stimulus dalam bentuk tayangan video mengenai cara monitoring lalu lintas jaringan di Mikrotik. [Video Monitoring Mikrotik](https://youtu.be/QlT5fEPhmBI) 3. Pendidik menjelaskan materi tentang fitur monitoring yang ada di Mikrotik, termasuk penggunaan tool seperti **Torch** dan **Traffic Flow** untuk menganalisis lalu lintas jaringan. 4. Pendidik memberikan referensi video yang menjelaskan cara monitoring jaringan menggunakan Mikrotik:    * [Menggunakan Torch untuk Monitoring Lalu Lintas Mikrotik](https://youtu.be/LE8AHJacCFM)    * Buku Elektronik Penunjang: [Panduan Monitoring Mikrotik](https://www.academia.edu/16832625/Pemrograman_web_statis_dan_dinamis) 5. Peserta didik melakukan latihan untuk menggunakan fitur **Torch** dan **Traffic Flow** di Mikrotik untuk memantau lalu lintas jaringan yang terjadi pada perangkat mereka. 6. Peserta didik diminta untuk mendiskusikan bagaimana menganalisis hasil monitoring untuk mendeteksi potensi masalah di jaringan, seperti kemacetan, penggunaan bandwidth yang   berlebihan, dan perangkat yang tidak sah.   1. Peserta didik menyusun dan merangkum langkah-langkah monitoring lalu lintas jaringan serta manfaatnya untuk pengelolaan jaringan yang lebih baik. 2. Masing-masing kelompok mempresentasikan hasil latihan dan diskusi mereka menggunakan media seperti PowerPoint, video tutorial, atau naskah cerita.   Pendidik meminta kelompok lain untuk memberikan tanggapan terhadap presentasi kelompok lainnya. |

|  |  |
| --- | --- |
| **Kegiatan**  **Pembelajaran** | **Deskripsi** |
|  | 1. Setiap kelompok mencatat masukan dan memperbaiki presentasi mereka. 2. Pendidik meminta kelompok untuk mengumpulkan hasil presentasi yang sudah disempurnakan sesuai media yang dipilih. |
| **Kegiatan Penutup (15 Menit)** | 1. Guru meminta siswa untuk mengisi refleksi pembelajaran melalui link yang disediakan. 2. Guru meminta perwakilan peserta didik memberikan refleksi pembelajaran hari ini. 3. Guru memberikan kesimpulan akhir dan meminta siswa yang sudah paham untuk membantu teman-teman yang masih belum memahami. 4. Guru menjelaskan materi minggu depan dan bahan yang perlu dipersiapkan siswa untuk kelancaran pembelajaran berikutnya. 5. Peserta didik dan pendidik mengakhiri pembelajaran dengan doa. |

Refleksi Peserta Didik

|  |  |  |  |
| --- | --- | --- | --- |
| **Pertanyaan Refleksi** | **Baik** | **Cukup** | **Kurang** |
| Apakah kalian sudah memahami cara menggunakan fitur **Torch** untuk monitoring lalu lintas jaringan? | [ ] | [ ] | [ ] |
| Apakah kalian sudah memahami cara menggunakan **Traffic Flow** di Mikrotik? | [ ] | [ ] | [ ] |
| Apakah kalian merasa lebih paham tentang pentingnya monitoring lalu lintas jaringan setelah pertemuan ini? | [ ] | [ ] | [ ] |
| Apakah kalian dapat menyebutkan potensi masalah yang dapat terdeteksi dengan monitoring lalu lintas jaringan? | [ ] | [ ] | [ ] |
| Apa yang masih kurang jelas mengenai cara menganalisis lalu lintas jaringan menggunakan Mikrotik? | [ ] | [ ] | [ ] |

Refleksi Pendidik

|  |  |  |
| --- | --- | --- |
| **No** | **Pertanyaan** | **Jawaban** |
| 1 | Apakah pemilihan media pembelajaran telah mencerminkan tujuan pembelajaran yang akan dicapai? | [ ] |
| 2 | Apakah gaya penyampaian materi mampu ditangkap oleh peserta didik? | [ ] |
| 3 | Apakah keseluruhan pembelajaran dapat memberikan makna pembelajaran yang hendak dicapai? | [ ] |
| 4 | Apakah pemilihan metode pembelajaran sudah efektif untuk menerjemahkan tujuan pembelajaran? | [ ] |
| 5 | Apakah pelaksanaan pelajaran hari ini dapat memberikan semangat kepada peserta didik untuk lebih antusias dalam pembelajaran selanjutnya? | [ ] |

Lampiran

* 1. **Lembar Kerja Peserta Didik**: Terlampir.
  2. **Pengayaan**: Untuk peserta didik yang hasil belajarnya belum mencapai target, pendidik melakukan pengulangan materi dengan pendekatan yang lebih individual dan memberikan tugas tambahan untuk memperbaiki hasil belajar peserta didik bersangkutan.

###### Bahan Bacaan Pendidik dan Peserta Didik:

Video tema "Monitoring Lalu Lintas Jaringan dengan Mikrotik": [Monitoring Mikrotik dengan Torch](https://youtu.be/LE8AHJacCFM). Buku Elektronik Penunjang Belajar: [Panduan Monitoring Mikrotik](https://www.academia.edu/16832625/Pemrograman_web_statis_dan_dinamis).

Glosarium

1. **Monitoring Lalu Lintas Jaringan**: Proses untuk memantau dan menganalisis data yang dikirim dan diterima dalam jaringan untuk memastikan lalu lintas berjalan lancar, mendeteksi masalah, dan menjaga performa jaringan.
2. **Torch**: Fitur di Mikrotik yang memungkinkan pengguna untuk memantau lalu lintas jaringan secara real-time, termasuk informasi tentang protokol, IP, dan port yang digunakan.
3. **Traffic Flow**: Fitur di Mikrotik yang digunakan untuk mengamati lalu lintas jaringan berdasarkan aliran data, membantu mengidentifikasi kemacetan atau penggunaan bandwidth yang tidak efisien.
4. **Bandwidth Utilization**: Penggunaan bandwidth pada jaringan yang mengukur seberapa banyak data yang dikirim atau diterima dalam waktu tertentu.

### Pertemuan Ketiga belas: Fitur-Fitur Keamanan pada Mikrotik\*\*

Kegiatan Pembelajaran

|  |  |
| --- | --- |
| **Kegiatan**  **Pembelajaran** | **Deskripsi** |
| **Pendahuluan (15 Menit)** | 1. Pendidik mengucapkan salam kepada peserta didik dan memulai kegiatan dengan membaca doa. 2. Pendidik melakukan presensi. 3. Pendidik memberikan kesempatan kepada beberapa peserta didik untuk membahas materi pertemuan sebelumnya tentang monitoring lalu lintas jaringan dengan Mikrotik. 4. Pendidik bersama dengan peserta didik menyepakati keyakinan kelas yang akan dilaksanakan selama pembelajaran. 5. Pendidik menyampaikan tujuan pembelajaran dan menyepakatinya dengan siswa. 6. Peserta didik diberikan pertanyaan pemantik, seperti:    1. Apa saja fitur keamanan yang perlu ada di Mikrotik?    2. Mengapa penting untuk mengamankan perangkat jaringan menggunakan Mikrotik? |
| **Kegiatan Inti (135 Menit)** | 1. Peserta didik dikelompokkan menjadi beberapa kelompok yang telah dibentuk di pertemuan sebelumnya. 2. Peserta didik diberikan stimulus dalam bentuk tayangan video mengenai fitur-fitur keamanan pada Mikrotik, seperti firewall, VPN, dan akses kontrol. [Video Fitur Keamanan Mikrotik](https://youtu.be/QlT5fEPhmBI) 3. Pendidik menjelaskan materi tentang berbagai fitur keamanan pada Mikrotik, termasuk:    * **Firewall** untuk melindungi jaringan dari ancaman luar    * **VPN** (Virtual Private Network) untuk akses aman ke jaringan    * **Hotspot Gateway** untuk kontrol akses internet    * **User Manager** untuk manajemen akses pengguna 4. Pendidik memberikan referensi video yang menjelaskan cara mengonfigurasi fitur keamanan di Mikrotik:    * [Mikrotik Firewall Configuration](https://youtu.be/LE8AHJacCFM)    * [VPN Setup on Mikrotik](https://youtu.be/pKJmb04T0FQ) 5. Peserta didik melakukan latihan konfigurasi fitur keamanan di Mikrotik, termasuk mengonfigurasi firewall, VPN, dan mengelola akses pengguna melalui **User Manager**. 6. Peserta didik mendiskusikan penerapan masing-masing fitur keamanan dalam skenario dunia nyata, seperti di perusahaan atau di rumah. 7. Peserta didik menyusun dan merangkum langkah-langkah konfigurasi keamanan Mikrotik serta manfaat yang diperoleh dari penggunaannya. 8. Masing-masing kelompok mempresentasikan hasil latihan dan diskusi mereka menggunakan media seperti PowerPoint, video tutorial, atau naskah cerita.   Pendidik meminta kelompok lain untuk memberikan tanggapan terhadap presentasi kelompok lainnya.   1. Setiap kelompok mencatat masukan dan memperbaiki presentasi mereka. 2. Pendidik meminta kelompok untuk mengumpulkan hasil presentasi yang sudah disempurnakan sesuai media yang dipilih. |
| **Kegiatan Penutup (15 Menit)** | 1. Guru meminta siswa untuk mengisi refleksi pembelajaran melalui link yang disediakan. 2. Guru meminta perwakilan peserta didik memberikan refleksi pembelajaran hari ini. 3. Guru memberikan kesimpulan akhir dan meminta siswa yang sudah paham untuk membantu teman-teman yang masih belum memahami. 4. Guru menjelaskan materi minggu depan dan bahan yang perlu dipersiapkan siswa untuk kelancaran pembelajaran berikutnya. 5. Peserta didik dan pendidik mengakhiri pembelajaran dengan doa. |

Refleksi Peserta Didik

|  |  |  |  |
| --- | --- | --- | --- |
| **Pertanyaan Refleksi** | **Baik** | **Cukup** | **Kurang** |
| Apakah kalian sudah memahami cara mengonfigurasi firewall pada Mikrotik? | [ ] | [ ] | [ ] |

|  |  |  |  |
| --- | --- | --- | --- |
| **Pertanyaan Refleksi** | **Baik** | **Cukup** | **Kurang** |
| Apakah kalian sudah memahami cara mengonfigurasi VPN pada Mikrotik? | [ ] | [ ] | [ ] |
| Apakah kalian merasa lebih paham tentang pengaturan fitur keamanan lainnya pada Mikrotik? | [ ] | [ ] | [ ] |
| Apakah kalian dapat menyebutkan langkah-langkah dasar dalam konfigurasi Hotspot dan User Manager? | [ ] | [ ] | [ ] |
| Apa yang masih kurang jelas mengenai penerapan fitur keamanan pada Mikrotik? | [ ] | [ ] | [ ] |

Refleksi Pendidik

|  |  |  |
| --- | --- | --- |
| **No** | **Pertanyaan** | **Jawaban** |
| 1 | Apakah pemilihan media pembelajaran telah mencerminkan tujuan pembelajaran yang akan dicapai? | [ ] |
| 2 | Apakah gaya penyampaian materi mampu ditangkap oleh peserta didik? | [ ] |
| 3 | Apakah keseluruhan pembelajaran dapat memberikan makna pembelajaran yang hendak dicapai? | [ ] |
| 4 | Apakah pemilihan metode pembelajaran sudah efektif untuk menerjemahkan tujuan pembelajaran? | [ ] |
| 5 | Apakah pelaksanaan pelajaran hari ini dapat memberikan semangat kepada peserta didik untuk lebih antusias dalam pembelajaran selanjutnya? | [ ] |

Lampiran

* 1. **Lembar Kerja Peserta Didik**: Terlampir.
  2. **Pengayaan**: Untuk peserta didik yang hasil belajarnya belum mencapai target, pendidik melakukan pengulangan materi dengan pendekatan yang lebih individual dan memberikan tugas tambahan untuk memperbaiki hasil belajar peserta didik bersangkutan.

###### Bahan Bacaan Pendidik dan Peserta Didik:

Video tema "Mengonfigurasi Fitur Keamanan Mikrotik": [Mikrotik Firewall](https://youtu.be/LE8AHJacCFM). Buku Elektronik Penunjang Belajar: [Panduan Mikrotik untuk Keamanan](https://www.academia.edu/16832625/Pemrograman_web_statis_dan_dinamis).

Glosarium

1. **Firewall Mikrotik**: Fitur keamanan pada Mikrotik yang berfungsi untuk memfilter dan mengontrol lalu lintas data yang masuk dan keluar dari jaringan.
2. **VPN Mikrotik**: Virtual Private Network yang memungkinkan koneksi aman melalui jaringan publik, sering digunakan untuk menghubungkan jaringan perusahaan dengan cabang atau pekerja jarak jauh.
3. **Hotspot Mikrotik**: Fitur yang memungkinkan untuk mengelola akses pengguna ke internet di area hotspot dengan memberikan otentikasi pengguna dan kontrol akses.
4. **User Manager Mikrotik**: Fitur Mikrotik untuk mengelola hak akses pengguna, memberikan autentikasi, dan membatasi akses ke sumber daya jaringan.

### Pertemuan Keempat belas: Analisis dan Optimalisasi Keamanan Jaringan\*\*

Kegiatan Pembelajaran

|  |  |
| --- | --- |
| **Kegiatan**  **Pembelajaran** | **Deskripsi** |
| **Pendahuluan (15 Menit)** | 1. Pendidik mengucapkan salam kepada peserta didik dan memulai kegiatan dengan membaca doa. 2. Pendidik melakukan presensi. 3. Pendidik memberikan kesempatan kepada beberapa peserta didik untuk membahas materi pertemuan sebelumnya tentang fitur keamanan pada Mikrotik. 4. Pendidik bersama dengan peserta didik menyepakati keyakinan kelas yang akan dilaksanakan selama pembelajaran. 5. Pendidik menyampaikan tujuan pembelajaran dan menyepakatinya dengan siswa. 6. Peserta didik diberikan pertanyaan pemantik, seperti: |

|  |  |
| --- | --- |
| **Kegiatan**  **Pembelajaran** | **Deskripsi** |
|  | 1. Apa yang dimaksud dengan optimalisasi keamanan jaringan? 2. Apa langkah-langkah yang perlu dilakukan untuk mengidentifikasi kelemahan dalam sistem keamanan jaringan? |
| **Kegiatan Inti (135 Menit)** | 1. Peserta didik dikelompokkan menjadi beberapa kelompok yang telah dibentuk di pertemuan sebelumnya. 2. Peserta didik diberikan stimulus dalam bentuk tayangan video mengenai cara menganalisis dan mengoptimalkan keamanan jaringan. [Video Analisis dan Optimalisasi Keamanan Jaringan](https://youtu.be/QlT5fEPhmBI) 3. Pendidik menjelaskan materi tentang analisis keamanan jaringan, termasuk langkah-langkah untuk mengidentifikasi kerentanannya, dan teknik untuk mengoptimalkan keamanan. 4. Pendidik memberikan referensi video yang menjelaskan analisis dan optimalisasi keamanan jaringan:    * [Analisis Keamanan Jaringan dan Best Practices](https://youtu.be/LE8AHJacCFM)    * Buku Elektronik Penunjang: [Panduan Keamanan Jaringan](https://www.academia.edu/16832625/Pemrograman_web_statis_dan_dinamis) 5. Peserta didik melakukan latihan untuk menganalisis konfigurasi keamanan jaringan yang ada dan mengidentifikasi potensi masalah atau titik lemah dalam pengaturan firewall, proxy, dan VPN yang telah diterapkan. 6. Peserta didik diminta untuk melakukan langkah-langkah optimalisasi untuk memperbaiki kelemahan yang ditemukan, termasuk menerapkan pembaruan keamanan, memperkuat kebijakan   akses, dan mengonfigurasi ulang firewall atau proxy sesuai dengan kebutuhan keamanan yang lebih tinggi.   1. Peserta didik mendiskusikan temuan dan solusi yang mereka usulkan, serta membuat rencana untuk mengimplementasikan solusi tersebut. 2. Peserta didik menyusun dan merangkum hasil analisis dan solusi optimalisasi keamanan jaringan mereka.   Masing-masing kelompok mempresentasikan hasil latihan dan diskusi mereka menggunakan media seperti PowerPoint, video tutorial, atau naskah cerita.   1. Pendidik meminta kelompok lain untuk memberikan tanggapan terhadap presentasi kelompok lainnya. 2. Setiap kelompok mencatat masukan dan memperbaiki presentasi mereka. 3. Pendidik meminta kelompok untuk mengumpulkan hasil presentasi yang sudah disempurnakan sesuai media yang dipilih. |
| **Kegiatan**  **Penutup (15 Menit)** | 1. Guru meminta siswa untuk mengisi refleksi pembelajaran melalui link yang disediakan. 2. Guru meminta perwakilan peserta didik memberikan refleksi pembelajaran hari ini. 3. Guru memberikan kesimpulan akhir dan meminta siswa yang sudah paham untuk membantu teman-teman yang masih belum memahami. 4. Guru menjelaskan materi minggu depan dan bahan yang perlu dipersiapkan siswa untuk kelancaran pembelajaran berikutnya. 5. Peserta didik dan pendidik mengakhiri pembelajaran dengan doa. |

Refleksi Peserta Didik

|  |  |  |  |
| --- | --- | --- | --- |
| **Pertanyaan Refleksi** | **Baik** | **Cukup** | **Kurang** |
| Apakah kalian sudah memahami langkah-langkah analisis keamanan jaringan? | [ ] | [ ] | [ ] |
| Apakah kalian sudah mengetahui cara mengoptimalkan pengaturan firewall dan proxy di jaringan? | [ ] | [ ] | [ ] |
| Apakah kalian merasa lebih paham tentang langkah-langkah untuk memperbaiki kerentanan keamanan setelah pertemuan ini? | [ ] | [ ] | [ ] |
| Apakah kalian dapat menyebutkan solusi yang efektif untuk mengoptimalkan keamanan jaringan? | [ ] | [ ] | [ ] |
| Apa yang masih kurang jelas mengenai optimalisasi dan analisis keamanan jaringan? | [ ] | [ ] | [ ] |

Refleksi Pendidik

|  |  |  |
| --- | --- | --- |
| **No** | **Pertanyaan** | **Jawaban** |
| 1 | Apakah pemilihan media pembelajaran telah mencerminkan tujuan pembelajaran yang akan dicapai? | [ ] |
| 2 | Apakah gaya penyampaian materi mampu ditangkap oleh peserta didik? | [ ] |

|  |  |  |
| --- | --- | --- |
| **No** | **Pertanyaan** | **Jawaban** |
| 3 | Apakah keseluruhan pembelajaran dapat memberikan makna pembelajaran yang hendak dicapai? | [ ] |
| 4 | Apakah pemilihan metode pembelajaran sudah efektif untuk menerjemahkan tujuan pembelajaran? | [ ] |
| 5 | Apakah pelaksanaan pelajaran hari ini dapat memberikan semangat kepada peserta didik untuk lebih antusias dalam pembelajaran selanjutnya? | [ ] |

Lampiran

1. **Lembar Kerja Peserta Didik**: Terlampir.
2. **Pengayaan**: Untuk peserta didik yang hasil belajarnya belum mencapai target, pendidik melakukan pengulangan materi dengan pendekatan yang lebih individual dan memberikan tugas tambahan untuk memperbaiki hasil belajar peserta didik bersangkutan.

###### Bahan Bacaan Pendidik dan Peserta Didik:

Video tema "Analisis dan Optimalisasi Keamanan Jaringan": [Optimalisasi Keamanan Jaringan](https://youtu.be/LE8AHJacCFM). Buku Elektronik Penunjang: [Panduan Keamanan Jaringan](https://www.academia.edu/16832625/Pemrograman_web_statis_dan_dinamis).

Glosarium

1. **Analisis Keamanan Jaringan**: Proses untuk mengidentifikasi kelemahan dan potensi ancaman dalam konfigurasi dan pengaturan sistem keamanan jaringan, seperti firewall, VPN, dan kebijakan akses.
2. **Optimalisasi Keamanan**: Langkah-langkah untuk memperbaiki atau meningkatkan pengaturan sistem keamanan

jaringan dengan memperkenalkan kontrol akses yang lebih ketat, memperbarui perangkat lunak, dan menerapkan teknik mitigasi ancaman.

1. **Kerentanan Keamanan**: Titik lemah dalam sistem yang dapat dieksploitasi oleh pihak yang tidak sah untuk mengakses atau merusak data dan sistem.
2. **Firewall**: Alat untuk memfilter dan mengontrol lalu lintas data yang masuk dan keluar dari jaringan untuk melindungi sistem dari serangan eksternal.
3. **Proxy Server**: Server yang bertindak sebagai perantara antara pengguna dan internet untuk meningkatkan keamanan dan kontrol akses.

### Pertemuan Kelima belas: Pengaturan Kebijakan Keamanan pada Mikrotik\*\*

Kegiatan Pembelajaran

|  |  |
| --- | --- |
| **Kegiatan**  **Pembelajaran** | **Deskripsi** |
| **Pendahuluan (15 Menit)** | 1. Pendidik mengucapkan salam kepada peserta didik dan memulai kegiatan dengan membaca doa. 2. Pendidik melakukan presensi. 3. Pendidik memberikan kesempatan kepada beberapa peserta didik untuk membahas materi pertemuan sebelumnya tentang analisis dan optimalisasi keamanan jaringan. 4. Pendidik bersama dengan peserta didik menyepakati keyakinan kelas yang akan dilaksanakan selama pembelajaran. 5. Pendidik menyampaikan tujuan pembelajaran dan menyepakatinya dengan siswa. 6. Peserta didik diberikan pertanyaan pemantik, seperti:    1. Apa itu kebijakan keamanan jaringan?    2. Bagaimana kebijakan keamanan dapat diterapkan di Mikrotik? |
| **Kegiatan Inti (135 Menit)** | 1. Peserta didik dikelompokkan menjadi beberapa kelompok yang telah dibentuk di pertemuan sebelumnya. 2. Peserta didik diberikan stimulus dalam bentuk tayangan video mengenai pengaturan kebijakan keamanan pada Mikrotik, seperti pengaturan firewall, VPN, dan kebijakan kontrol akses. [Video](https://youtu.be/QlT5fEPhmBI)   [Pengaturan Kebijakan Keamanan Mikrotik](https://youtu.be/QlT5fEPhmBI)   1. Pendidik menjelaskan materi tentang kebijakan keamanan yang dapat diterapkan pada Mikrotik, termasuk pengaturan:    * **Firewall** untuk melindungi jaringan dari ancaman luar.    * **VPN** untuk memastikan koneksi yang aman. |

|  |  |
| --- | --- |
| **Kegiatan**  **Pembelajaran** | **Deskripsi** |
|  | - **User Manager** untuk mengatur kebijakan akses dan hak pengguna.   1. Pendidik memberikan referensi video yang menjelaskan cara mengonfigurasi kebijakan keamanan di Mikrotik:    * [Pengaturan Firewall Mikrotik](https://youtu.be/LE8AHJacCFM)    * [Mikrotik VPN Configuration](https://youtu.be/pKJmb04T0FQ) 2. Peserta didik melakukan latihan konfigurasi kebijakan keamanan pada Mikrotik, termasuk   pengaturan firewall untuk kontrol akses, VPN untuk keamanan koneksi jarak jauh, dan pengaturan kebijakan akses pengguna dengan **User Manager**.   1. Peserta didik diminta untuk mendiskusikan dan menganalisis implementasi kebijakan keamanan dalam skenario dunia nyata, seperti pada jaringan perusahaan atau sekolah. 2. Peserta didik menyusun dan merangkum langkah-langkah pengaturan kebijakan keamanan di Mikrotik serta manfaat yang diperoleh dari penerapannya. 3. Masing-masing kelompok mempresentasikan hasil latihan dan diskusi mereka menggunakan media seperti PowerPoint, video tutorial, atau naskah cerita.   Pendidik meminta kelompok lain untuk memberikan tanggapan terhadap presentasi kelompok lainnya.   1. Setiap kelompok mencatat masukan dan memperbaiki presentasi mereka. 2. Pendidik meminta kelompok untuk mengumpulkan hasil presentasi yang sudah disempurnakan sesuai media yang dipilih. |
| **Kegiatan Penutup (15 Menit)** | 1. Guru meminta siswa untuk mengisi refleksi pembelajaran melalui link yang disediakan. 2. Guru meminta perwakilan peserta didik memberikan refleksi pembelajaran hari ini. 3. Guru memberikan kesimpulan akhir dan meminta siswa yang sudah paham untuk membantu teman-teman yang masih belum memahami. 4. Guru menjelaskan materi minggu depan dan bahan yang perlu dipersiapkan siswa untuk kelancaran pembelajaran berikutnya. 5. Peserta didik dan pendidik mengakhiri pembelajaran dengan doa. |

Refleksi Peserta Didik

|  |  |  |  |
| --- | --- | --- | --- |
| **Pertanyaan Refleksi** | **Baik** | **Cukup** | **Kurang** |
| Apakah kalian sudah memahami cara mengonfigurasi kebijakan keamanan di Mikrotik? | [ ] | [ ] | [ ] |
| Apakah kalian sudah memahami cara mengonfigurasi firewall untuk kontrol akses di Mikrotik? | [ ] | [ ] | [ ] |
| Apakah kalian sudah mengetahui cara mengonfigurasi VPN di Mikrotik untuk keamanan koneksi? | [ ] | [ ] | [ ] |
| Apakah kalian dapat menyebutkan langkah-langkah dasar dalam pengaturan kebijakan akses pengguna di Mikrotik? | [ ] | [ ] | [ ] |
| Apa yang masih kurang jelas mengenai pengaturan kebijakan keamanan di Mikrotik? | [ ] | [ ] | [ ] |

Refleksi Pendidik

|  |  |  |
| --- | --- | --- |
| **No** | **Pertanyaan** | **Jawaban** |
| 1 | Apakah pemilihan media pembelajaran telah mencerminkan tujuan pembelajaran yang akan dicapai? | [ ] |
| 2 | Apakah gaya penyampaian materi mampu ditangkap oleh peserta didik? | [ ] |
| 3 | Apakah keseluruhan pembelajaran dapat memberikan makna pembelajaran yang hendak dicapai? | [ ] |
| 4 | Apakah pemilihan metode pembelajaran sudah efektif untuk menerjemahkan tujuan pembelajaran? | [ ] |
| 5 | Apakah pelaksanaan pelajaran hari ini dapat memberikan semangat kepada peserta didik untuk lebih antusias dalam pembelajaran selanjutnya? | [ ] |

Lampiran

* 1. **Lembar Kerja Peserta Didik**: Terlampir.
  2. **Pengayaan**: Untuk peserta didik yang hasil belajarnya belum mencapai target, pendidik melakukan pengulangan materi dengan pendekatan yang lebih individual dan memberikan tugas tambahan untuk memperbaiki hasil belajar peserta didik bersangkutan.

###### Bahan Bacaan Pendidik dan Peserta Didik:

Video tema "Pengaturan Kebijakan Keamanan Mikrotik": [Pengaturan Firewall Mikrotik](https://youtu.be/LE8AHJacCFM). Buku Elektronik Penunjang Belajar: [Panduan Keamanan Mikrotik](https://www.academia.edu/16832625/Pemrograman_web_statis_dan_dinamis).

Glosarium

1. **Kebijakan Keamanan**: Serangkaian aturan yang diterapkan untuk melindungi data, perangkat, dan sumber daya di dalam jaringan. Ini mencakup pengaturan akses, pengelolaan perangkat keras dan perangkat lunak, serta kontrol terhadap komunikasi di jaringan.
2. **Firewall Mikrotik**: Alat di Mikrotik yang digunakan untuk mengontrol akses ke jaringan dengan memfilter lalu lintas berdasarkan aturan tertentu.
3. **VPN Mikrotik**: Virtual Private Network di Mikrotik memungkinkan koneksi yang aman antara jaringan lokal dan jaringan luar (seperti internet) melalui saluran terenkripsi.
4. **User Manager Mikrotik**: Fitur Mikrotik untuk mengelola hak akses pengguna, memungkinkan admin untuk menetapkan izin yang tepat dan membatasi akses ke sumber daya tertentu dalam jaringan.

### Pertemuan Keenam belas: Praktik Deteksi dan Mitigasi Ancaman dengan Mikrotik\*\*

Kegiatan Pembelajaran

|  |  |
| --- | --- |
| **Kegiatan**  **Pembelajaran** | **Deskripsi** |
| **Pendahuluan (15 Menit)** | 1. Pendidik mengucapkan salam kepada peserta didik dan memulai kegiatan dengan membaca doa. 2. Pendidik melakukan presensi. 3. Pendidik memberikan kesempatan kepada beberapa peserta didik untuk membahas materi pertemuan sebelumnya tentang pengaturan kebijakan keamanan pada Mikrotik. 4. Pendidik bersama dengan peserta didik menyepakati keyakinan kelas yang akan dilaksanakan selama pembelajaran. 5. Pendidik menyampaikan tujuan pembelajaran dan menyepakatinya dengan siswa. 6. Peserta didik diberikan pertanyaan pemantik, seperti:    1. Apa itu mitigasi ancaman dalam keamanan jaringan?    2. Mengapa deteksi dan mitigasi ancaman sangat penting dalam pengelolaan jaringan? |
| **Kegiatan Inti (135 Menit)** | 1. Peserta didik dikelompokkan menjadi beberapa kelompok yang telah dibentuk di pertemuan sebelumnya. 2. Peserta didik diberikan stimulus dalam bentuk tayangan video mengenai cara mendeteksi dan melakukan mitigasi ancaman menggunakan Mikrotik. [Video Deteksi dan Mitigasi Ancaman Mikrotik](https://youtu.be/QlT5fEPhmBI) 3. Pendidik menjelaskan materi tentang cara mendeteksi ancaman jaringan, seperti serangan DDoS, port scanning, dan akses tidak sah. Pendidik juga menjelaskan teknik mitigasi yang bisa diterapkan di Mikrotik, termasuk penggunaan firewall, filter, dan tools monitoring seperti **Torch** dan **Traffic Flow**. 4. Pendidik memberikan referensi video yang menjelaskan teknik deteksi dan mitigasi ancaman di Mikrotik:    * [Deteksi dan Mitigasi Ancaman dengan Mikrotik](https://youtu.be/LE8AHJacCFM)    * [Firewall Mikrotik untuk Mitigasi Ancaman](https://youtu.be/pKJmb04T0FQ) 5. Peserta didik melakukan latihan untuk mendeteksi ancaman di jaringan menggunakan **Torch** dan **Traffic Flow** di Mikrotik, serta memitigasi ancaman dengan mengonfigurasi firewall dan fitur keamanan lainnya. 6. Peserta didik diminta untuk mengidentifikasi ancaman yang mereka temui selama latihan dan memberikan solusi mitigasi yang tepat. 7. Peserta didik mendiskusikan cara-cara untuk memperkuat pertahanan jaringan dengan mengidentifikasi potensi celah dan merencanakan langkah-langkah mitigasi yang lebih efektif. 8. Peserta didik menyusun dan merangkum hasil latihan deteksi ancaman dan mitigasi yang mereka lakukan.   Masing-masing kelompok mempresentasikan hasil latihan dan diskusi mereka menggunakan media seperti PowerPoint, video tutorial, atau naskah cerita.   1. Pendidik meminta kelompok lain untuk memberikan tanggapan terhadap presentasi kelompok lainnya. 2. Setiap kelompok mencatat masukan dan memperbaiki presentasi mereka. |

|  |  |
| --- | --- |
| **Kegiatan**  **Pembelajaran** | **Deskripsi** |
|  | 12. Pendidik meminta kelompok untuk mengumpulkan hasil presentasi yang sudah disempurnakan  sesuai media yang dipilih. |
| **Kegiatan**  **Penutup (15 Menit)** | 1. Guru meminta siswa untuk mengisi refleksi pembelajaran melalui link yang disediakan. 2. Guru meminta perwakilan peserta didik memberikan refleksi pembelajaran hari ini. 3. Guru memberikan kesimpulan akhir dan meminta siswa yang sudah paham untuk membantu teman-teman yang masih belum memahami. 4. Guru menjelaskan materi minggu depan dan bahan yang perlu dipersiapkan siswa untuk kelancaran pembelajaran berikutnya. 5. Peserta didik dan pendidik mengakhiri pembelajaran dengan doa. |

Refleksi Peserta Didik

|  |  |  |  |
| --- | --- | --- | --- |
| **Pertanyaan Refleksi** | **Baik** | **Cukup** | **Kurang** |
| Apakah kalian sudah memahami cara mendeteksi ancaman menggunakan Mikrotik? | [ ] | [ ] | [ ] |
| Apakah kalian sudah memahami cara memitigasi ancaman menggunakan firewall Mikrotik? | [ ] | [ ] | [ ] |
| Apakah kalian merasa lebih paham tentang langkah-langkah mitigasi ancaman setelah pertemuan ini? | [ ] | [ ] | [ ] |
| Apakah kalian dapat menyebutkan beberapa jenis ancaman yang dapat dideteksi menggunakan Mikrotik? | [ ] | [ ] | [ ] |
| Apa yang masih kurang jelas mengenai deteksi dan mitigasi ancaman dengan Mikrotik? | [ ] | [ ] | [ ] |

Refleksi Pendidik

|  |  |  |
| --- | --- | --- |
| **No** | **Pertanyaan** | **Jawaban** |
| 1 | Apakah pemilihan media pembelajaran telah mencerminkan tujuan pembelajaran yang akan dicapai? | [ ] |
| 2 | Apakah gaya penyampaian materi mampu ditangkap oleh peserta didik? | [ ] |
| 3 | Apakah keseluruhan pembelajaran dapat memberikan makna pembelajaran yang hendak dicapai? | [ ] |
| 4 | Apakah pemilihan metode pembelajaran sudah efektif untuk menerjemahkan tujuan pembelajaran? | [ ] |
| 5 | Apakah pelaksanaan pelajaran hari ini dapat memberikan semangat kepada peserta didik untuk lebih antusias dalam pembelajaran selanjutnya? | [ ] |

Lampiran

* 1. **Lembar Kerja Peserta Didik**: Terlampir.
  2. **Pengayaan**: Untuk peserta didik yang hasil belajarnya belum mencapai target, pendidik melakukan pengulangan materi dengan pendekatan yang lebih individual dan memberikan tugas tambahan untuk memperbaiki hasil belajar peserta didik bersangkutan.

###### Bahan Bacaan Pendidik dan Peserta Didik:

Video tema "Deteksi dan Mitigasi Ancaman dengan Mikrotik": [Deteksi Ancaman Mikrotik](https://youtu.be/LE8AHJacCFM). Buku Elektronik Penunjang Belajar: [Panduan Keamanan Mikrotik](https://www.academia.edu/16832625/Pemrograman_web_statis_dan_dinamis).

Glosarium

1. **Deteksi Ancaman**: Proses untuk mengidentifikasi potensi ancaman atau serangan terhadap jaringan, termasuk melalui analisis trafik jaringan dan penggunaan alat seperti **Torch** dan **Traffic Flow** pada Mikrotik.
2. **Mitigasi Ancaman**: Langkah-langkah yang diambil untuk mengurangi atau menghilangkan ancaman yang terdeteksi di jaringan, seperti menerapkan aturan firewall, menggunakan VPN, atau memperbarui perangkat lunak untuk mengatasi kerentanannya.
3. **DDoS (Distributed Denial of Service)**: Jenis serangan yang dilakukan dengan membanjiri sistem atau jaringan dengan trafik yang berlebihan untuk membuat layanan tidak dapat diakses.
4. **Port Scanning**: Teknik yang digunakan oleh penyerang untuk mencari port terbuka pada perangkat jaringan untuk mengeksploitasi kerentanannya.

### Pertemuan Ketujuh belas: Review dan Ujian Praktek Firewall & Proxy\*\*

Kegiatan Pembelajaran

|  |  |
| --- | --- |
| **Kegiatan**  **Pembelajaran** | **Deskripsi** |
| **Pendahuluan (15 Menit)** | 1. Pendidik mengucapkan salam kepada peserta didik dan memulai kegiatan dengan membaca doa. 2. Pendidik melakukan presensi. 3. Pendidik memberikan kesempatan kepada beberapa peserta didik untuk merefleksikan materi sebelumnya tentang pengaturan dan pengelolaan firewall serta proxy. 4. Pendidik bersama dengan peserta didik menyepakati keyakinan kelas yang akan dilaksanakan selama pembelajaran. 5. Pendidik menyampaikan tujuan pembelajaran dan menyepakatinya dengan siswa. 6. Peserta didik diberikan pertanyaan pemantik, seperti:    1. Apa saja jenis firewall yang telah dipelajari?    2. Apa saja manfaat penggunaan proxy server dalam jaringan? |
| **Kegiatan Inti (135 Menit)** | 1. Pendidik melakukan review singkat mengenai konsep-konsep yang telah dipelajari tentang firewall dan proxy. 2. Peserta didik diberikan stimulus berupa latihan soal dan kasus untuk menguji pemahaman mereka mengenai firewall, proxy, serta penerapannya dalam jaringan. 3. Pendidik menjelaskan langkah-langkah yang harus diambil dalam ujian praktek, yang mencakup konfigurasi firewall dan proxy pada Mikrotik dan Ubuntu. 4. Pendidik memberikan referensi video dan dokumentasi untuk membantu peserta didik mengingat materi yang telah dipelajari:    * [Konfigurasi Firewall Mikrotik](https://youtu.be/LE8AHJacCFM)    * [Pengaturan Proxy Server Mikrotik dan Ubuntu](https://youtu.be/pKJmb04T0FQ) 5. Peserta didik mengerjakan ujian praktek yang mencakup konfigurasi firewall, pengaturan proxy, serta penerapan kebijakan keamanan di jaringan. 6. Pendidik memberikan waktu untuk peserta didik melakukan konfigurasi dan menyelesaikan ujian praktek mereka secara individu atau dalam kelompok. 7. Pendidik berkeliling untuk memantau dan memberikan bantuan jika diperlukan selama ujian praktek. 8. Peserta didik diminta untuk menyelesaikan ujian praktek sesuai dengan instruksi yang   diberikan, termasuk pengaturan firewall untuk kontrol akses dan proxy untuk mengelola lalu lintas internet.  Setelah ujian praktek, peserta didik diminta untuk mempresentasikan hasil konfigurasi dan solusi yang diterapkan selama ujian. |
| **Kegiatan Penutup (15 Menit)** | 1. Guru meminta siswa untuk mengisi refleksi pembelajaran melalui link yang disediakan. 2. Guru meminta perwakilan peserta didik memberikan refleksi pembelajaran hari ini dan pengalaman selama ujian praktek. 3. Guru memberikan kesimpulan akhir mengenai topik yang telah dibahas, serta memberi umpan balik tentang ujian praktek. 4. Guru memberikan informasi mengenai materi dan bahan yang perlu dipersiapkan siswa untuk pembelajaran selanjutnya. 5. Peserta didik dan pendidik mengakhiri pembelajaran dengan doa. |

Refleksi Peserta Didik

|  |  |  |  |
| --- | --- | --- | --- |
| **Pertanyaan Refleksi** | **Baik** | **Cukup** | **Kurang** |
| Apakah kalian merasa cukup siap untuk mengonfigurasi firewall dan proxy setelah ujian praktek ini? | [ ] | [ ] | [ ] |
| Apakah kalian sudah memahami langkah-langkah yang benar dalam mengonfigurasi firewall dan proxy? | [ ] | [ ] | [ ] |
| Apakah kalian dapat menerapkan konsep yang telah dipelajari pada skenario dunia nyata? | [ ] | [ ] | [ ] |

|  |  |  |  |
| --- | --- | --- | --- |
| **Pertanyaan Refleksi** | **Baik** | **Cukup** | **Kurang** |
| Apa yang kalian anggap sulit selama ujian praktek ini dan bagaimana cara mengatasinya? | [ ] | [ ] | [ ] |
| Apakah kalian merasa lebih percaya diri dalam mengelola firewall dan proxy di jaringan setelah ujian ini? | [ ] | [ ] | [ ] |

Refleksi Pendidik

|  |  |  |
| --- | --- | --- |
| **No** | **Pertanyaan** | **Jawaban** |
| 1 | Apakah pemilihan media pembelajaran telah mencerminkan tujuan pembelajaran yang akan dicapai? | [ ] |
| 2 | Apakah gaya penyampaian materi mampu ditangkap oleh peserta didik? | [ ] |
| 3 | Apakah keseluruhan pembelajaran dapat memberikan makna pembelajaran yang hendak dicapai? | [ ] |
| 4 | Apakah pemilihan metode pembelajaran sudah efektif untuk menerjemahkan tujuan pembelajaran? | [ ] |
| 5 | Apakah pelaksanaan pelajaran hari ini dapat memberikan semangat kepada peserta didik untuk lebih antusias dalam pembelajaran selanjutnya? | [ ] |

Lampiran

* 1. **Lembar Kerja Peserta Didik**: Terlampir.
  2. **Pengayaan**: Untuk peserta didik yang hasil belajarnya belum mencapai target, pendidik melakukan pengulangan materi dengan pendekatan yang lebih individual dan memberikan tugas tambahan untuk memperbaiki hasil belajar peserta didik bersangkutan.

###### Bahan Bacaan Pendidik dan Peserta Didik:

Video tema "Pengaturan Firewall dan Proxy Mikrotik": [Pengaturan Firewall Mikrotik](https://youtu.be/LE8AHJacCFM). Buku Elektronik Penunjang Belajar: [Panduan Firewall dan Proxy Mikrotik](https://www.academia.edu/16832625/Pemrograman_web_statis_dan_dinamis).

Glosarium

1. **Firewall Mikrotik**: Alat di Mikrotik untuk memfilter dan mengontrol lalu lintas data yang masuk dan keluar dari jaringan, melindungi sistem dari serangan eksternal.
2. **Proxy Server**: Server yang digunakan sebagai perantara untuk mengelola akses antara pengguna dan internet, sering digunakan untuk meningkatkan keamanan dan mempercepat akses.
3. **Kontrol Akses**: Pengaturan yang digunakan untuk membatasi atau mengizinkan akses ke sumber daya tertentu dalam jaringan berdasarkan kriteria tertentu, seperti alamat IP, protokol, atau jenis layanan.
4. **VPN (Virtual Private Network)**: Jaringan pribadi yang memungkinkan pengaksesan aman melalui internet dengan menggunakan enkripsi untuk menjaga kerahasiaan data.

### Pertemuan Kedelapan belas: Refleksi dan Kesimpulan Semester\*\*

Kegiatan Pembelajaran

|  |  |
| --- | --- |
| **Kegiatan**  **Pembelajaran** | **Deskripsi** |
| **Pendahuluan (15 Menit)** | 1. Pendidik mengucapkan salam kepada peserta didik dan memulai kegiatan dengan membaca doa. 2. Pendidik melakukan presensi. 3. Pendidik memberikan kesempatan kepada beberapa peserta didik untuk merefleksikan materi yang telah dipelajari sepanjang semester. 4. Pendidik bersama dengan peserta didik menyepakati keyakinan kelas yang akan dilaksanakan selama pembelajaran. 5. Pendidik menyampaikan tujuan pembelajaran hari ini yaitu untuk merefleksikan hasil belajar semester dan menyusun kesimpulan pembelajaran. 6. Peserta didik diberikan pertanyaan pemantik, seperti: |

|  |  |
| --- | --- |
| **Kegiatan**  **Pembelajaran** | **Deskripsi** |
|  | 1. Apa yang paling berkesan dari pembelajaran semester ini? 2. Apa tantangan terbesar yang dihadapi dalam mempelajari materi terkait keamanan jaringan? |
| **Kegiatan Inti (135 Menit)** | 1. Pendidik meminta peserta didik untuk merefleksikan dan mendiskusikan materi yang telah dipelajari selama semester ini, mulai dari dasar keamanan jaringan, konfigurasi firewall, proxy, hingga mitigasi ancaman. 2. Peserta didik diminta untuk menulis dan mendiskusikan pengalaman mereka mengenai   penerapan konsep-konsep yang telah dipelajari, serta bagaimana mereka mengatasi tantangan yang dihadapi.   1. Pendidik mengajak peserta didik untuk membahas solusi dan perbaikan yang dapat diterapkan pada pengelolaan keamanan jaringan di dunia nyata. 2. Peserta didik menyusun kesimpulan mengenai apa yang telah mereka pelajari dan seberapa pentingnya topik-topik tersebut untuk pengelolaan jaringan yang aman. 3. Pendidik memberikan kesempatan kepada setiap kelompok untuk mempresentasikan kesimpulan mereka mengenai pembelajaran yang telah dilakukan, mencakup topik yang paling penting dan cara-cara untuk mengatasi tantangan yang ada. 4. Pendidik memberikan umpan balik terhadap hasil refleksi dan presentasi kelompok. 5. Pendidik memberikan klarifikasi dan memperkuat pemahaman peserta didik mengenai materi yang perlu dipahami lebih dalam. 6. Peserta didik mengajukan pertanyaan atau berbagi pengalaman mereka selama semester terkait materi pembelajaran. |
| **Kegiatan Penutup (15 Menit)** | 1. Guru meminta siswa untuk mengisi refleksi pembelajaran melalui link yang disediakan. 2. Guru meminta perwakilan peserta didik untuk memberikan refleksi tentang pengalaman pembelajaran semester ini. 3. Guru memberikan kesimpulan akhir tentang pembelajaran yang telah dilaksanakan selama semester, serta memberikan umpan balik terhadap perkembangan dan pencapaian peserta didik. 4. Guru memberikan informasi mengenai materi tambahan atau referensi untuk studi lanjutan terkait keamanan jaringan. 5. Peserta didik dan pendidik mengakhiri pembelajaran dengan doa. |

Refleksi Peserta Didik

|  |  |  |  |
| --- | --- | --- | --- |
| **Pertanyaan Refleksi** | **Baik** | **Cukup** | **Kurang** |
| Apa yang paling kalian sukai dari pembelajaran semester ini? | [ ] | [ ] | [ ] |
| Apa tantangan terbesar yang kalian hadapi selama mempelajari keamanan jaringan? | [ ] | [ ] | [ ] |
| Apakah kalian merasa lebih siap dalam mengelola keamanan jaringan setelah semester ini? | [ ] | [ ] | [ ] |
| Apa yang paling berkesan dan bermanfaat dari pembelajaran firewall dan proxy? | [ ] | [ ] | [ ] |
| Apa yang masih perlu kalian pelajari lebih lanjut untuk memperdalam pemahaman tentang keamanan jaringan? | [ ] | [ ] | [ ] |

Refleksi Pendidik

|  |  |  |
| --- | --- | --- |
| **No** | **Pertanyaan** | **Jawaban** |
| 1 | Apakah pemilihan media pembelajaran telah mencerminkan tujuan pembelajaran yang akan dicapai? | [ ] |
| 2 | Apakah gaya penyampaian materi mampu ditangkap oleh peserta didik? | [ ] |
| 3 | Apakah keseluruhan pembelajaran dapat memberikan makna pembelajaran yang hendak dicapai? | [ ] |
| 4 | Apakah pemilihan metode pembelajaran sudah efektif untuk menerjemahkan tujuan pembelajaran? | [ ] |
| 5 | Apakah pelaksanaan pelajaran hari ini dapat memberikan semangat kepada peserta didik untuk lebih antusias dalam pembelajaran selanjutnya? | [ ] |

Lampiran

* 1. **Lembar Kerja Peserta Didik**: Terlampir.
  2. **Pengayaan**: Untuk peserta didik yang hasil belajarnya belum mencapai target, pendidik melakukan pengulangan materi dengan pendekatan yang lebih individual dan memberikan tugas tambahan untuk memperbaiki hasil belajar peserta didik

bersangkutan.

###### Bahan Bacaan Pendidik dan Peserta Didik:

Video tema "Membangun Keamanan Jaringan yang Kuat": [Keamanan Jaringan dan Firewall](https://youtu.be/LE8AHJacCFM). Buku Elektronik Penunjang: [Panduan Keamanan Jaringan](https://www.academia.edu/16832625/Pemrograman_web_statis_dan_dinamis).

Glosarium

1. **Keamanan Jaringan**: Upaya untuk melindungi jaringan komputer dari ancaman yang dapat mengakses, merusak, atau mencuri data. Ini mencakup pengaturan firewall, pengelolaan akses, dan proteksi terhadap serangan eksternal.
2. **Firewall**: Alat di jaringan yang digunakan untuk memfilter dan mengontrol lalu lintas data yang masuk dan keluar, berdasarkan aturan yang telah ditetapkan untuk mencegah akses yang tidak sah.
3. **Proxy Server**: Server yang bertindak sebagai perantara antara pengguna dan server lainnya di internet, sering digunakan untuk meningkatkan keamanan, mengatur kontrol akses, dan mempercepat koneksi.
4. **Mitigasi Ancaman**: Langkah-langkah yang diambil untuk mengurangi atau menghilangkan ancaman terhadap jaringan, seperti menggunakan firewall dan VPN untuk memperkuat keamanan.

# \*\*C. Lampiran

#### Lembar Kerja Peserta Didik (LKPD)

LKPD 1: Pengantar Firewall

##### Tujuan Pembelajaran**:**

Peserta didik memahami definisi dan fungsi firewall dalam menjaga keamanan jaringan. Peserta didik mengenali jenis-jenis firewall (Hardware, Software, Stateful, Stateless).

##### Instruksi Kerja**:**

* 1. Bacalah teori dasar tentang firewall pada modul pembelajaran.
  2. Tonton video pengantar tentang firewall yang telah disediakan melalui tautan [Pengantar Firewall](https://youtu.be/QlT5fEPhmBI).
  3. Diskusikan dengan kelompok:

Apa fungsi utama firewall dalam jaringan?

Apa saja jenis-jenis firewall (Hardware, Software, Stateful, Stateless)?

* 1. Kerjakan soal berikut:

Jelaskan secara ringkas pengertian firewall.

Sebutkan tiga contoh penerapan firewall dalam jaringan.

##### Langkah Praktikum**:**

1. **Studi Kasus**: Analisis kebutuhan keamanan pada jaringan kecil (rumah/kantor kecil). Tentukan jenis firewall yang sesuai.
2. Presentasikan hasil diskusi kelompok dengan visualisasi sederhana (gambar/skema).

##### Hasil yang Diharapkan**:**

Peserta dapat menjelaskan konsep firewall secara jelas.

Peserta mampu memberikan contoh penerapan firewall berdasarkan jenisnya.

LKPD 2: Arsitektur dan Desain Firewall

##### Tujuan Pembelajaran**:**

Memahami struktur desain arsitektur firewall dalam jaringan. Memilih desain firewall yang sesuai dengan kebutuhan.

##### Instruksi Kerja**:**

1. Pelajari berbagai jenis arsitektur firewall, seperti DMZ, single-layer, dan multi-layer.
2. Diskusikan dalam kelompok:

Apa kelebihan DMZ dibandingkan dengan single-layer firewall?

Dalam skenario jaringan sekolah, jenis arsitektur apa yang paling cocok?

1. Kerjakan soal berikut:

Jelaskan perbedaan antara arsitektur firewall DMZ dan single-layer.

Bagaimana Anda memilih arsitektur firewall yang sesuai untuk jaringan perusahaan?

##### Langkah Praktikum**:**

1. Buat diagram arsitektur jaringan sederhana untuk: DMZ

Single-layer firewall Multi-layer firewall

1. Bandingkan manfaat dan kekurangan setiap desain.

##### Hasil yang Diharapkan**:**

Peserta memahami desain firewall dan memilih arsitektur yang sesuai dengan kebutuhan jaringan.

LKPD 3: Packet Filtering dengan Mikrotik

##### Tujuan Pembelajaran**:**

Memahami konsep packet filtering.

Menerapkan konfigurasi packet filtering dasar pada router Mikrotik untuk pengendalian lalu lintas.

##### Instruksi Kerja**:**

1. Pelajari konsep packet filtering dan cara kerja pada router Mikrotik.
2. Gunakan **RouterOS** atau **Virtual Lab** untuk konfigurasi.
3. Kerjakan soal berikut:

Jelaskan apa yang dimaksud dengan packet filtering dalam firewall.

Sebutkan langkah-langkah untuk mengonfigurasi packet filtering pada Mikrotik.

##### Langkah Praktikum**:**

1. Buka antarmuka Mikrotik melalui **WinBox** atau terminal.
2. Masukkan aturan berikut:

Drop paket dari IP tertentu (misal: 192.168.1.10).

Allow paket untuk port tertentu (misal: port 80 untuk HTTP).

1. Uji hasil dengan mengakses port yang diizinkan dan yang diblokir.

##### Hasil yang Diharapkan**:**

Peserta memahami cara kerja packet filtering dan mampu mengonfigurasi aturan dasar.

LKPD 4: Konfigurasi dan Pengelolaan Firewall

##### Tujuan Pembelajaran**:**

Mengonfigurasi aturan firewall untuk mengontrol lalu lintas jaringan. Memahami pengelolaan kebijakan akses pada firewall.

##### Instruksi Kerja**:**

1. Pelajari cara membuat kebijakan firewall untuk: Membatasi akses pengguna tertentu. Mengatur waktu akses (time-based rules).
2. Simulasikan skenario: Batasi akses ke server internal dari jaringan luar.

##### Langkah Praktikum**:**

1. Buat aturan pada Mikrotik untuk:

Memblokir akses dari subnet tertentu (misal: 192.168.2.0/24) ke server 192.168.1.100. Membatasi akses hanya pada jam 08:00-17:00.

1. Uji hasil konfigurasi dengan mencoba akses dari IP yang diblokir.

##### Hasil yang Diharapkan**:**

Peserta mampu mengatur aturan firewall untuk kebijakan akses tertentu.

LKPD 5: Monitor dan Log Aktivitas Firewall

##### Tujuan Pembelajaran**:**

Memahami pentingnya monitoring dan logging pada firewall. Menganalisis log aktivitas firewall untuk mendeteksi ancaman.

##### Instruksi Kerja**:**

1. Aktifkan logging pada Mikrotik untuk semua trafik yang mencurigakan.
2. Analisis log untuk:

Deteksi port scanning. Deteksi akses ilegal.

##### Langkah Praktikum**:**

1. Gunakan fitur logging pada Mikrotik dengan perintah:

/ip firewall filter add chain=input action=log log-prefix="LOG\_TEST"

1. Simulasikan port scanning dengan **Nmap**.
2. Periksa log di Mikrotik dan catat aktivitas mencurigakan.

##### Hasil yang Diharapkan**:**

Peserta dapat membaca log firewall dan memahami cara mendeteksi ancaman.

LKPD 6: Implementasi Firewall dalam Jaringan

##### Tujuan Pembelajaran**:**

Mempraktikkan konfigurasi firewall pada jaringan perusahaan. Menyusun kebijakan keamanan jaringan.

##### Instruksi Kerja**:**

1. Konfigurasikan firewall pada Mikrotik untuk mengizinkan akses hanya ke server tertentu.
2. Buat kebijakan yang membatasi akses ke server internal dari jaringan luar.

##### Langkah Praktikum**:**

1. Terapkan aturan firewall:

Allow traffic ke server 192.168.1.50 pada port 22 (SSH). Block semua traffic lain.

1. Uji koneksi dari IP luar ke server.

##### Hasil yang Diharapkan**:**

Peserta dapat mengimplementasikan kebijakan firewall dalam jaringan.

LKPD 7: Tantangan dan Tren Terbaru dalam Firewall

##### Tujuan Pembelajaran**:**

Mengenali tantangan terkini dalam keamanan jaringan.

Memahami konsep **Next-Generation Firewall (NGFW)** dan kelebihannya.

##### Instruksi Kerja**:**

1. Pelajari perbedaan antara NGFW dan firewall tradisional.
2. Diskusikan skenario integrasi NGFW dengan IDS/IPS.

##### Langkah Praktikum**:**

1. Simulasikan penggunaan fitur NGFW, seperti inspeksi mendalam paket data (DPI).
2. Diskusikan skenario implementasi NGFW di jaringan perusahaan.

##### Hasil yang Diharapkan**:**

Peserta memahami konsep NGFW dan kelebihannya.

LKPD 8: Pengantar Proxy Server

##### Tujuan Pembelajaran**:**

Memahami definisi dan fungsi proxy server.

Mengenali jenis-jenis proxy server dan penggunaannya.

##### Instruksi Kerja**:**

1. Bacalah materi tentang proxy server, jenis-jenisnya (forward, reverse, transparent).
2. Diskusikan dengan kelompok:

Apa perbedaan antara proxy server dan firewall?

Sebutkan manfaat utama proxy server dalam jaringan.

##### Langkah Praktikum**:**

1. Tonton video pengantar proxy server.
2. Buat diagram alur kerja proxy server pada jaringan kecil (contoh: kantor).
3. Diskusikan skenario penggunaan proxy server di jaringan sekolah.

##### Hasil yang Diharapkan**:**

Peserta mampu menjelaskan peran proxy server dalam keamanan jaringan. Peserta memahami jenis-jenis proxy dan penggunaannya.

LKPD 9: Proxy Internal dengan Mikrotik

##### Tujuan Pembelajaran**:**

Mengonfigurasi proxy internal pada router Mikrotik. Mengelola kebijakan akses melalui proxy internal.

##### Instruksi Kerja**:**

1. Pelajari konfigurasi dasar proxy internal pada Mikrotik.
2. Gunakan **WinBox** untuk mengaktifkan fitur proxy di Mikrotik.
3. Kerjakan soal berikut:

Jelaskan bagaimana cara mengonfigurasi proxy internal pada Mikrotik.

Sebutkan beberapa manfaat menggunakan proxy internal dalam jaringan.

##### Langkah Praktikum**:**

1. Aktifkan fitur **web proxy** di Mikrotik dengan perintah:

/ip proxy set enabled=yes

1. Tambahkan aturan untuk memblokir akses ke domain tertentu:

/ip proxy access add dst-host=[www.example.com](http://www.example.com/) action=deny

1. Uji dengan mencoba mengakses domain yang diblokir.

##### Hasil yang Diharapkan**:**

Peserta dapat mengatur kebijakan akses menggunakan proxy internal di Mikrotik.

LKPD 10: Proxy Eksternal dengan Ubuntu

##### Tujuan Pembelajaran**:**

Menginstal dan mengonfigurasi proxy server eksternal menggunakan Ubuntu. Memahami pengelolaan kebijakan akses melalui Squid Proxy.

##### Instruksi Kerja**:**

1. Instal Squid Proxy pada Ubuntu dengan perintah:

sudo apt install squid

1. Konfigurasikan Squid Proxy untuk: Membatasi akses ke situs tertentu.

Mengatur cache untuk meningkatkan kecepatan akses.

##### Langkah Praktikum**:**

1. Edit file konfigurasi Squid:

sudo nano /etc/squid/squid.conf

Tambahkan aturan untuk memblokir domain tertentu:

acl blocksite dstdomain .example.com http\_access deny blocksite

1. Restart Squid Proxy:

sudo systemctl restart squid

1. Uji hasil dengan mencoba mengakses domain yang diblokir.

##### Hasil yang Diharapkan**:**

Peserta dapat mengonfigurasi proxy eksternal menggunakan Squid Proxy di Ubuntu.

LKPD 11: Pengaturan Kebijakan Proxy Server

##### Tujuan Pembelajaran**:**

Mengatur kebijakan akses melalui proxy server. Membatasi akses berdasarkan waktu atau jenis konten.

##### Instruksi Kerja**:**

1. Pelajari fitur pembatasan akses pada proxy server.
2. Diskusikan skenario untuk:

Membatasi akses selama jam tertentu. Mengizinkan akses hanya ke situs edukasi.

##### Langkah Praktikum**:**

1. Konfigurasikan kebijakan waktu akses di Squid Proxy:

acl workhours time MTWHF 08:00-17:00 http\_access allow workhours

1. Tambahkan aturan untuk mengizinkan akses ke situs tertentu:

acl edu\_sites dstdomain .edu http\_access allow edu\_sites

1. Uji hasil dengan mencoba akses di luar jam kerja.

##### Hasil yang Diharapkan**:**

Peserta mampu menerapkan kebijakan akses berbasis waktu dan konten.

LKPD 12: Monitoring Lalu Lintas Jaringan dengan Mikrotik

##### Tujuan Pembelajaran**:**

Memahami fungsi monitoring pada perangkat Mikrotik untuk keamanan jaringan.

Menggunakan fitur monitoring Mikrotik untuk mengawasi lalu lintas jaringan secara real-time dan mendeteksi aktivitas mencurigakan.

##### Instruksi Kerja**:**

1. Pelajari fitur **torch** pada Mikrotik untuk monitoring lalu lintas.
2. Kerjakan soal berikut:

Jelaskan bagaimana fitur torch digunakan untuk memonitor trafik di jaringan.

Apa jenis aktivitas yang dapat dideteksi menggunakan fitur monitoring Mikrotik?

##### Langkah Praktikum**:**

1. Buka **WinBox** dan navigasikan ke **Tools > Torch**.
2. Pilih interface yang ingin dipantau dan klik **Start**.
3. Catat IP atau port dengan trafik mencurigakan dan analisis hasilnya.

##### Hasil yang Diharapkan**:**

Peserta dapat menggunakan fitur monitoring Mikrotik untuk mendeteksi aktivitas mencurigakan dan memahami data yang diperoleh.

LKPD 13: Fitur-Fitur Keamanan pada Mikrotik

##### Tujuan Pembelajaran**:**

Mengenal fitur keamanan yang tersedia di Mikrotik, seperti firewall, NAT, dan logging. Mengonfigurasi fitur-fitur keamanan tersebut pada Mikrotik untuk proteksi jaringan.

##### Instruksi Kerja**:**

1. Pelajari fungsi masing-masing fitur keamanan pada Mikrotik.
2. Kerjakan soal berikut:

Jelaskan apa saja fitur keamanan yang ada pada Mikrotik dan bagaimana cara mengonfigurasinya. Sebutkan manfaat dari pengaturan NAT pada Mikrotik.

##### Langkah Praktikum**:**

1. Tambahkan aturan NAT untuk akses internet:

/ip firewall nat add chain=srcnat action=masquerade out-interface=ether1

1. Aktifkan logging untuk mencatat trafik tertentu:

/ip firewall filter add chain=forward action=log

##### Hasil yang Diharapkan**:**

Peserta memahami dan mampu mengonfigurasi fitur keamanan dasar di Mikrotik.

LKPD 14: Analisis dan Optimalisasi Keamanan Jaringan

##### Tujuan Pembelajaran**:**

Menggunakan data monitoring untuk analisis dan optimalisasi. Membuat kebijakan keamanan yang lebih efektif.

##### Instruksi Kerja**:**

1. Analisis hasil monitoring untuk: Identifikasi potensi ancaman.

Rekomendasi optimalisasi keamanan.

##### Langkah Praktikum**:**

1. Gunakan fitur **Log** dan **Torch** untuk mengumpulkan data.
2. Buat kebijakan untuk:

Memblokir IP dengan trafik mencurigakan. Membatasi bandwidth untuk aplikasi tertentu.

##### Hasil yang Diharapkan**:**

Peserta dapat menganalisis dan mengoptimalkan keamanan jaringan dengan kebijakan yang tepat.

LKPD 15: Pengaturan Kebijakan Keamanan pada Mikrotik

##### Tujuan Pembelajaran**:**

Menyusun kebijakan keamanan berdasarkan hasil analisis. Menerapkan kebijakan untuk melindungi jaringan.

##### Instruksi Kerja**:**

1. Buat kebijakan untuk:

Membatasi akses berdasarkan IP.

Mengatur prioritas bandwidth untuk aplikasi penting.

##### Langkah Praktikum**:**

1. Tambahkan aturan firewall untuk memblokir akses tertentu:

/ip firewall filter add chain=forward src-address=192.168.1.50 action=drop

1. Uji hasil dengan mencoba akses dari IP yang diblokir.

##### Hasil yang Diharapkan**:**

Peserta mampu menerapkan kebijakan keamanan pada Mikrotik.

LKPD 16: Praktik Deteksi dan Mitigasi Ancaman dengan Mikrotik

##### Tujuan Pembelajaran**:**

Mendeteksi ancaman seperti DDoS dan malware. Menerapkan mitigasi ancaman dengan Mikrotik.

##### Instruksi Kerja**:**

1. Simulasikan serangan DDoS menggunakan **hping3**.
2. Buat aturan firewall untuk membatasi trafik:

/ip firewall filter add chain=input protocol=tcp connection-limit=100,32 action=drop

##### Hasil yang Diharapkan**:**

Peserta mampu mendeteksi dan memitigasi ancaman pada jaringan dengan Mikrotik.

LKPD 17: Review dan Ujian Praktik Firewall & Proxy

##### Tujuan Pembelajaran**:**

Menguasai konfigurasi firewall dan proxy secara menyeluruh. Melakukan praktik ujian untuk mengevaluasi pemahaman.

##### Instruksi Kerja**:**

1. Lakukan konfigurasi berikut:

Firewall untuk membatasi akses.

Proxy untuk membatasi situs tertentu.

Langkah Praktikum**:**

1. Praktikkan semua konfigurasi yang telah dipelajari dalam simulasi ujian.

##### Hasil yang Diharapkan**:**

Peserta dapat menyelesaikan ujian praktik dengan baik dan memahami semua konsep yang telah dipelajari.

LKPD 18: Refleksi dan Kesimpulan Semester

##### Tujuan Pembelajaran**:**

Merefleksikan hasil pembelajaran selama semester.

Menyusun rekomendasi untuk pengelolaan keamanan jaringan di masa depan.

##### Instruksi Kerja**:**

1. Diskusikan dengan kelompok:

Apa hal paling sulit dalam konfigurasi firewall/proxy?

Rekomendasi apa yang dapat diberikan untuk peningkatan keamanan jaringan?

##### Langkah Praktikum**:**

1. Tulis laporan refleksi tentang apa yang telah dipelajari selama semester.
2. Diskusikan kesimpulan dan masukan untuk pengelolaan keamanan jaringan yang lebih baik.

##### Hasil yang Diharapkan**:**

Peserta mampu merefleksikan dan menyimpulkan pembelajaran dengan baik.

#### Lampiran Penilaian

* 1. Penilaian Pengetahuan

**Mata Pelajaran**: Sistem Keamanan Jaringan

**Bentuk Soal**: Pilihan Ganda **Kelas/Semester**: XI / Genap **Jumlah Soal**: 50

**Nama Guru**: Idiarso, S.Kom

##### Tujuan Penilaian

Penilaian pengethuan ini bertujuan untuk mengukur tingkat pemahaman, kemampuan analisis, dan keterampilan peserta didik dalam mengimplementasikan konsep-konsep yang telah dipelajari terkait **Sistem keamanan jaringan**, khususnya pada

penerapan **firewall**, **proxy server**, dan **pengelolaan jaringan** menggunakan Mikrotik dan Ubuntu. Tujuan spesifik penilaian ini meliputi:

###### Pemahaman Konseptual

Mengukur sejauh mana peserta didik memahami: Definisi, fungsi, dan jenis-jenis firewall.

Fungsi proxy server dan perbedaannya dengan firewall.

Komponen dan fitur penting dalam pengelolaan keamanan jaringan.

###### Kemampuan Teknis dan Praktis

Menguji kemampuan peserta didik untuk:

Melakukan konfigurasi firewall dan proxy server menggunakan Mikrotik dan Ubuntu. Mengelola fitur keamanan seperti packet filtering, NAT, port forwarding, dan log monitoring.

Mengimplementasikan kebijakan akses, pengelolaan bandwidth, dan filtering konten melalui perangkat jaringan.

###### Analisis dan Pemecahan Masalah

Menilai kemampuan peserta didik dalam:

Menganalisis masalah keamanan jaringan seperti serangan siber atau ancaman internal.

Mengidentifikasi dan menerapkan solusi yang efektif untuk melindungi jaringan menggunakan perangkat dan teknik yang dipelajari.

Mengevaluasi dan mengoptimalkan konfigurasi keamanan berdasarkan kebutuhan jaringan tertentu.

###### Penerapan Teknologi Terkait

Menilai penerapan teknologi jaringan seperti:

Penggunaan Mikrotik untuk manajemen lalu lintas data dan keamanan jaringan. Konfigurasi Squid Proxy di Ubuntu untuk pengelolaan akses internet.

Integrasi firewall dan proxy server untuk meningkatkan efisiensi dan perlindungan jaringan.

###### Etika dan Tanggung Jawab

Mengukur pemahaman peserta didik tentang:

Pentingnya menjaga integritas, kerahasiaan, dan keamanan data di jaringan. Penerapan prinsip etika dalam pengelolaan sistem keamanan jaringan.

Kesadaran terhadap tanggung jawab dalam mengelola keamanan jaringan yang sesuai dengan standar profesional.

##### Capaian yang Diharapkan

Setelah mengikuti penilaian ini, peserta didik diharapkan mampu:

Memahami konsep dasar dan fungsi keamanan jaringan, termasuk firewall dan proxy server.

Menerapkan konfigurasi perangkat jaringan seperti Mikrotik dan Ubuntu secara tepat untuk melindungi jaringan dari ancaman.

Menganalisis skenario keamanan jaringan dan memberikan solusi yang relevan serta efektif. Menunjukkan sikap profesional, etis, dan bertanggung jawab dalam pengelolaan keamanan jaringan.

##### Soal

###### Apersepsi

Firewall berfungsi sebagai pengontrol utama lalu lintas data dalam jaringan. Ia memeriksa data masuk dan keluar berdasarkan aturan yang telah ditetapkan, sehingga melindungi jaringan dari ancaman seperti virus dan serangan siber.

###### Soal

Apa fungsi utama firewall dalam jaringan?

1. Menghubungkan perangkat dalam jaringan
2. Mengontrol lalu lintas jaringan sesuai aturan yang ditentukan
3. Mempercepat koneksi internet
4. Memantau aktivitas pengguna di jaringan
5. Membatasi penggunaan data aplikasi tertentu

**ANS**: B

###### Apersepsi

Jenis-jenis firewall dapat berupa perangkat keras atau perangkat lunak, masing-masing memiliki kelebihan dan kekurangan. Firewall perangkat keras biasanya digunakan pada jaringan besar untuk mengontrol akses secara terpusat.

###### Soal

Apa kelebihan utama firewall berbasis perangkat keras?

1. Mudah diinstalasi pada perangkat apa pun
2. Memberikan proteksi terpusat untuk seluruh jaringan
3. Memiliki biaya yang lebih murah dibanding perangkat lunak
4. Mempercepat akses internet
5. Tidak membutuhkan konfigurasi tambahan

**ANS**: B

###### Apersepsi

Firewall berbasis perangkat lunak sering digunakan untuk kebutuhan individu atau jaringan kecil. Firewall ini biasanya terintegrasi langsung pada sistem operasi atau perangkat tertentu.

###### Soal

Apa kelemahan utama firewall berbasis perangkat lunak?

1. Tidak dapat diinstal pada perangkat tertentu
2. Membutuhkan perangkat keras tambahan
3. Beban pada sistem komputer yang menjalankan firewall meningkat
4. Tidak bisa memonitor lalu lintas jaringan
5. Tidak bisa digunakan dalam jaringan lokal

**ANS**: C

###### Apersepsi

Packet filtering adalah teknik dasar pada firewall yang memeriksa data berdasarkan header paket, seperti alamat IP atau nomor port. Teknik ini digunakan untuk menyaring lalu lintas data sesuai aturan yang telah ditentukan.

###### Soal

Apa yang diperiksa dalam packet filtering firewall?

1. Isi data pada paket
2. Header paket, seperti alamat IP dan nomor port
3. Lokasi fisik perangkat di jaringan
4. Riwayat akses perangkat
5. Jenis aplikasi yang digunakan

**ANS**: B

###### Apersepsi

Stateful firewall melacak status koneksi aktif untuk memastikan bahwa setiap paket data sesuai dengan koneksi yang sedang berlangsung. Teknologi ini meningkatkan keamanan dibandingkan firewall stateless.

###### Soal

Apa perbedaan utama antara stateful firewall dan stateless firewall?

1. Stateless firewall lebih kompleks dibanding stateful firewall
2. Stateful firewall melacak status koneksi, sedangkan stateless firewall tidak
3. Stateless firewall membutuhkan lebih banyak sumber daya dibanding stateful firewall
4. Stateful firewall hanya digunakan untuk jaringan lokal
5. Stateless firewall tidak mendukung aturan filtering

**ANS**: B

###### Apersepsi

Proxy server dapat digunakan untuk menyembunyikan alamat IP asli pengguna, meningkatkan keamanan privasi, dan membatasi akses ke konten tertentu.

###### Soal

Apa fungsi utama dari proxy server?

1. Mengganti perangkat firewall dalam jaringan
2. Menyembunyikan alamat IP pengguna untuk privasi dan keamanan
3. Mempercepat koneksi internet dengan mengelola bandwidth
4. Memblokir semua akses ke jaringan internet
5. Mengelola perangkat dalam jaringan lokal

**ANS**: B

###### Apersepsi

Desain arsitektur firewall sangat penting untuk menentukan seberapa efektif perlindungan yang diberikan pada jaringan. Arsitektur firewall dapat mencakup zona DMZ (Demilitarized Zone) untuk melindungi server dari ancaman luar.

###### Soal

Apa tujuan utama zona DMZ dalam arsitektur firewall?

1. Mempercepat pengiriman data
2. Menyediakan area aman bagi server yang terhubung ke internet
3. Menghubungkan perangkat internal secara langsung dengan jaringan eksternal
4. Menghapus ancaman malware secara otomatis
5. Memfilter lalu lintas yang masuk berdasarkan isi data

**ANS**: B

###### Apersepsi

Firewall dapat dirancang untuk memisahkan jaringan internal dari jaringan eksternal. Salah satu pendekatan desain adalah dual-homed firewall, yang memiliki dua interface jaringan.

###### Soal

Apa keunggulan utama dari dual-homed firewall?

1. Meningkatkan kecepatan jaringan internal
2. Memisahkan jaringan internal dan eksternal secara fisik
3. Tidak memerlukan konfigurasi tambahan untuk pengamanan
4. Menghapus kebutuhan akan enkripsi data
5. Mengizinkan semua lalu lintas tanpa filter

**ANS**: B

###### Apersepsi

Konfigurasi packet filtering pada Mikrotik memungkinkan pengguna untuk menentukan aturan yang memblokir atau mengizinkan lalu lintas data berdasarkan parameter tertentu, seperti alamat IP dan port.

###### Soal

Apa langkah pertama dalam konfigurasi packet filtering pada Mikrotik?

1. Menentukan perangkat tujuan
2. Menentukan aturan firewall berdasarkan alamat IP atau port
3. Mengatur bandwidth pengguna
4. Memperbarui sistem operasi router
5. Memindahkan perangkat ke DMZ

**ANS**: B

###### Apersepsi

Logging aktivitas firewall adalah fitur penting untuk memantau lalu lintas data di jaringan. Log ini mencatat semua aktivitas, termasuk upaya akses yang berhasil atau diblokir.

###### Soal

Apa manfaat utama dari fitur logging pada firewall?

1. Menghapus ancaman secara otomatis
2. Meningkatkan kecepatan koneksi jaringan
3. Mencatat dan menganalisis aktivitas jaringan untuk mendeteksi ancaman
4. Mengurangi penggunaan bandwidth perangkat tertentu
5. Menghubungkan perangkat langsung ke jaringan eksternal

**ANS**: C

###### Apersepsi

Next-Generation Firewall (NGFW) adalah evolusi dari firewall tradisional. NGFW menawarkan kemampuan tambahan, seperti inspeksi paket mendalam (DPI) dan deteksi ancaman berbasis aplikasi.

###### Soal

Apa keunggulan utama dari Next-Generation Firewall dibandingkan firewall tradisional?

1. Menggunakan lebih sedikit sumber daya
2. Menyediakan konektivitas antarperangkat secara langsung
3. Menawarkan deteksi ancaman berbasis aplikasi
4. Menghilangkan kebutuhan akan enkripsi data
5. Tidak memerlukan konfigurasi tambahan

**ANS**: C

###### Apersepsi

Proxy internal biasanya digunakan dalam jaringan lokal untuk mengontrol akses pengguna ke internet. Proxy ini juga dapat menyimpan data cache untuk mempercepat akses ke situs web yang sering dikunjungi.

###### Soal

Apa fungsi utama dari proxy internal?

1. Mengontrol akses pengguna ke sumber daya eksternal
2. Menyaring data yang berasal dari internet ke jaringan lokal
3. Mempercepat koneksi internet dengan mengelola bandwidth
4. Menghubungkan jaringan lokal langsung ke internet
5. Menghapus data pengguna secara otomatis

**ANS**: A

###### Apersepsi

Proxy eksternal biasanya digunakan untuk mengelola lalu lintas data dari jaringan internal ke internet. Proxy ini membantu menyembunyikan alamat IP internal dari jaringan eksternal.

###### Soal

Apa manfaat utama dari menggunakan proxy eksternal?

1. Mengelola cache untuk mempercepat akses ke situs lokal
2. Menyembunyikan alamat IP internal dari jaringan eksternal
3. Menghapus ancaman malware pada perangkat internal
4. Mempercepat akses data di jaringan lokal
5. Mengurangi jumlah perangkat yang terhubung ke jaringan

**ANS**: B

###### Apersepsi

Squid Proxy adalah perangkat lunak open-source yang sering digunakan untuk mengatur proxy eksternal. Squid Proxy memungkinkan administrator untuk mengelola cache, kontrol akses, dan filter konten.

###### Soal

Apa langkah pertama dalam konfigurasi Squid Proxy pada Ubuntu?

1. Membatasi bandwidth pengguna
2. Menginstal perangkat lunak Squid Proxy
3. Membuat aturan firewall untuk semua perangkat
4. Mengatur log aktivitas jaringan
5. Mengaktifkan mode transparan pada proxy

**ANS**: B

###### Apersepsi

Pengaturan kebijakan proxy server mencakup pembatasan akses ke situs tertentu dan pengelolaan bandwidth untuk meningkatkan efisiensi jaringan.

###### Soal

Apa yang dimaksud dengan kebijakan proxy server?

1. Aturan untuk mengatur akses jaringan eksternal melalui proxy
2. Prosedur untuk mempercepat koneksi internet
3. Kebijakan untuk menghubungkan perangkat langsung ke jaringan internal
4. Pengaturan yang menyimpan data pengguna di log
5. Proses menghapus ancaman malware secara otomatis

**ANS**: A

Saya akan melanjutkan dengan format yang sama hingga mencapai 50 soal. Jika ada preferensi khusus, beri tahu saya! Berikut adalah kelanjutan soal hingga mencapai 50:

###### Apersepsi

Logging pada proxy server sangat penting untuk menganalisis pola akses pengguna dan mendeteksi aktivitas yang mencurigakan.

###### Soal

Apa tujuan utama dari logging pada proxy server?

1. Mempercepat koneksi ke situs tertentu
2. Mencatat aktivitas pengguna untuk analisis dan keamanan
3. Mengurangi bandwidth pengguna jaringan
4. Menghapus data cache secara otomatis
5. Menyimpan log secara permanen tanpa batas waktu

**ANS**: B

###### Apersepsi

Dalam konfigurasi proxy server, filter konten digunakan untuk membatasi akses ke situs tertentu berdasarkan kategori atau kata kunci.

###### Soal

Apa manfaat utama dari filter konten pada proxy server?

1. Mempercepat akses situs web tertentu
2. Membatasi akses pengguna ke situs web tertentu berdasarkan aturan
3. Meningkatkan koneksi langsung ke jaringan eksternal
4. Menghapus ancaman malware di perangkat
5. Mengizinkan semua lalu lintas tanpa pembatasan

**ANS**: B

###### Apersepsi

Fitur monitoring di Mikrotik memungkinkan administrator jaringan untuk memantau lalu lintas secara real-time dan mendeteksi aktivitas mencurigakan.

###### Soal

Apa fitur utama dari monitoring pada perangkat Mikrotik?

1. Memblokir semua akses jaringan secara otomatis
2. Menghapus log lama pada router
3. Memantau lalu lintas jaringan secara real-time
4. Mempercepat transfer data antar perangkat
5. Menghubungkan perangkat secara langsung ke internet

**ANS**: C

###### Apersepsi

Analisis lalu lintas jaringan menggunakan perangkat Mikrotik penting untuk mendeteksi potensi ancaman dan mengoptimalkan penggunaan bandwidth.

###### Soal

Apa langkah pertama dalam analisis lalu lintas jaringan menggunakan Mikrotik?

1. Memeriksa konektivitas perangkat ke internet
2. Mengatur aturan firewall berdasarkan kebutuhan
3. Mengaktifkan fitur logging dan monitoring
4. Menyusun kebijakan akses pengguna
5. Membatasi penggunaan bandwidth secara manual

**ANS**: C

###### Apersepsi

Next-Generation Firewall (NGFW) memiliki kemampuan untuk mendeteksi ancaman berbasis aplikasi dan memblokir serangan yang tidak dapat dideteksi oleh firewall tradisional.

###### Soal

Apa fitur tambahan yang dimiliki oleh NGFW dibandingkan firewall tradisional?

1. Pengelolaan bandwidth yang lebih efisien
2. Deteksi ancaman berbasis aplikasi dan inspeksi mendalam
3. Penghapusan semua ancaman secara otomatis
4. Penyimpanan log tanpa batas waktu
5. Integrasi dengan perangkat lokal tanpa konfigurasi

**ANS**: B

###### Apersepsi

Konfigurasi VPN pada Mikrotik memungkinkan pengguna untuk terhubung ke jaringan secara aman dari lokasi yang berbeda.

###### Soal

Apa keuntungan utama menggunakan VPN pada jaringan Mikrotik?

1. Mempercepat akses data antar perangkat
2. Memungkinkan koneksi aman ke jaringan internal dari jarak jauh
3. Menghapus ancaman malware secara otomatis
4. Memblokir semua lalu lintas data masuk
5. Membatasi bandwidth pengguna di jaringan lokal

**ANS**: B

###### Apersepsi

Proxy internal sering digunakan untuk mengontrol akses pengguna dalam jaringan lokal dan meningkatkan efisiensi melalui caching.

###### Soal

Apa perbedaan utama antara proxy internal dan eksternal?

1. Proxy internal mengontrol akses dalam jaringan lokal, sedangkan proxy eksternal mengelola akses dari jaringan luar ke dalam
2. Proxy internal digunakan untuk mempercepat akses internet, sedangkan proxy eksternal untuk memperlambat akses
3. Proxy internal membutuhkan perangkat keras tambahan, sedangkan proxy eksternal tidak
4. Proxy internal memantau aktivitas pengguna, sedangkan proxy eksternal tidak
5. Proxy internal hanya bekerja dengan cache, sedangkan proxy eksternal tidak

**ANS**: A

###### Apersepsi

Pengaturan kebijakan keamanan jaringan mencakup kontrol akses pengguna dan pembatasan layanan tertentu untuk meningkatkan keamanan.

###### Soal

Apa langkah pertama dalam menyusun kebijakan keamanan jaringan?

1. Menentukan perangkat yang akan digunakan
2. Mengidentifikasi kebutuhan dan risiko keamanan jaringan
3. Memblokir semua akses yang tidak dikenal
4. Memperbarui perangkat lunak keamanan
5. Menghapus data pengguna lama

**ANS**: B

###### Apersepsi

Mikrotik menyediakan fitur firewall, proxy, dan logging untuk melindungi jaringan dari ancaman dan mengontrol lalu lintas data.

###### Soal

Apa fungsi utama fitur firewall pada Mikrotik?

1. Menyimpan data pengguna secara aman
2. Mengontrol lalu lintas data sesuai aturan yang ditentukan
3. Mempercepat koneksi perangkat lokal
4. Menghapus ancaman secara otomatis
5. Menyimpan log lalu lintas tanpa batas waktu

**ANS**: B

###### Apersepsi

Firewall stateless tidak melacak status koneksi, sehingga setiap paket data diperiksa secara individual berdasarkan aturan yang telah ditentukan.

###### Soal

Apa kelemahan utama firewall stateless?

1. Tidak dapat memeriksa setiap paket data
2. Membutuhkan lebih banyak sumber daya dibanding firewall stateful
3. Tidak melacak status koneksi, sehingga kurang aman
4. Hanya bekerja untuk jaringan lokal kecil
5. Tidak dapat mengontrol akses pengguna

**ANS**: C

###### Apersepsi

Dalam jaringan yang kompleks, penggunaan firewall berbasis perangkat keras memberikan keunggulan dalam kinerja karena tidak membebani server.

###### Soal

Apa kelebihan utama dari firewall berbasis perangkat keras dibandingkan firewall berbasis perangkat lunak?

1. Lebih murah dan mudah diakses
2. Memiliki kapasitas penyimpanan lebih besar
3. Tidak membebani kinerja perangkat utama
4. Tidak memerlukan pembaruan perangkat lunak
5. Dapat digunakan tanpa konfigurasi tambahan

**ANS**: C

###### Apersepsi

Packet filtering adalah fitur pada firewall yang memungkinkan penyaringan lalu lintas data berdasarkan alamat IP, port, atau protokol tertentu.

###### Soal

Apa manfaat utama dari konfigurasi packet filtering?

1. Menghapus ancaman malware secara otomatis
2. Membatasi lalu lintas berdasarkan parameter yang ditentukan
3. Menyimpan data log dalam jumlah besar
4. Mempercepat koneksi internet melalui filtering
5. Menghubungkan perangkat secara langsung ke jaringan

**ANS**: B

###### Apersepsi

Proxy server transparan memungkinkan pengguna untuk mengakses jaringan tanpa perlu melakukan konfigurasi di sisi klien.

###### Soal

Apa keunggulan utama dari proxy transparan?

1. Mempercepat koneksi dengan menyimpan cache
2. Tidak memerlukan konfigurasi tambahan di sisi pengguna
3. Menghapus data pengguna lama secara otomatis
4. Membatasi akses ke perangkat internal
5. Mengontrol bandwidth untuk semua pengguna

**ANS**: B

###### Apersepsi

Squid Proxy adalah perangkat lunak yang sering digunakan untuk membangun proxy server yang efisien dan fleksibel.

###### Soal

Apa langkah penting dalam pengaturan Squid Proxy untuk membatasi akses ke situs tertentu?

1. Menyimpan data pengguna dalam log
2. Menambahkan aturan ACL (Access Control List)
3. Mempercepat koneksi dengan cache otomatis
4. Memblokir semua lalu lintas dari perangkat tertentu
5. Menghapus data situs dari cache

**ANS**: B

###### Apersepsi

Konfigurasi firewall pada Mikrotik memungkinkan pengguna untuk menetapkan aturan berdasarkan alamat IP, port, dan protokol.

###### Soal

Apa fungsi utama dari "chain" dalam pengaturan firewall Mikrotik?

1. Menghubungkan dua perangkat secara langsung
2. Mengatur urutan eksekusi aturan firewall
3. Mempercepat akses data antar perangkat
4. Menyimpan log aktivitas jaringan
5. Menghapus ancaman secara otomatis

**ANS**: B

###### Apersepsi

Dalam jaringan modern, penggunaan VPN menjadi solusi utama untuk menghubungkan pengguna jarak jauh dengan jaringan internal secara aman.

###### Soal

Apa prinsip kerja utama dari Virtual Private Network (VPN)?

1. Mempercepat koneksi jaringan lokal
2. Mengenkripsi data untuk menjaga keamanan saat terkoneksi ke jaringan publik
3. Menghubungkan perangkat langsung ke internet
4. Memblokir lalu lintas dari alamat IP tertentu
5. Membatasi akses pengguna ke jaringan tertentu

**ANS**: B

###### Apersepsi

Analisis lalu lintas jaringan dengan menggunakan fitur monitoring pada Mikrotik membantu mendeteksi pola penggunaan data yang mencurigakan.

###### Soal

Apa tujuan utama dari analisis lalu lintas jaringan?

1. Mempercepat akses ke internet
2. Mendeteksi ancaman dan mengoptimalkan penggunaan sumber daya jaringan
3. Menghapus data pengguna yang tidak aktif
4. Membatasi akses pengguna tertentu
5. Menghubungkan perangkat langsung ke jaringan eksternal

**ANS**: B

###### Apersepsi

Firewall stateful memiliki keunggulan dibandingkan firewall stateless karena dapat melacak status koneksi dan pola lalu lintas data.

###### Soal

Apa peran utama dari fitur stateful inspection pada firewall?

1. Menyimpan data log dalam jumlah besar
2. Melacak status koneksi untuk memastikan validitas data
3. Mempercepat transfer data antar perangkat
4. Menghapus ancaman malware secara otomatis
5. Menghubungkan perangkat langsung ke internet

**ANS**: B

###### Apersepsi

Integrasi antara proxy server dan IDS/IPS (Intrusion Detection/Prevention System) memberikan lapisan perlindungan tambahan untuk jaringan.

###### Soal

Apa manfaat utama dari integrasi proxy server dengan IDS/IPS?

1. Mempercepat akses internet
2. Mendeteksi dan mencegah ancaman berdasarkan pola lalu lintas
3. Menghapus ancaman malware pada perangkat internal
4. Mengontrol bandwidth pengguna jaringan lokal
5. Menghubungkan perangkat langsung ke jaringan eksternal

**ANS**: B

###### Apersepsi

Kebijakan keamanan pada proxy server dirancang untuk membatasi akses pengguna ke situs tertentu dan mengontrol penggunaan bandwidth.

###### Soal

Apa langkah pertama dalam menyusun kebijakan keamanan pada proxy server?

1. Menentukan perangkat yang akan digunakan
2. Menyusun daftar situs yang akan dibatasi
3. Mengidentifikasi kebutuhan dan risiko keamanan jaringan
4. Memperbarui perangkat lunak keamanan
5. Menghapus data pengguna lama

**ANS**: C

###### Apersepsi

Proxy internal sering digunakan untuk mengelola dan memantau lalu lintas jaringan lokal dengan lebih efektif.

###### Soal

Apa keuntungan utama menggunakan proxy internal dalam jaringan lokal?

1. Mempercepat koneksi antar perangkat lokal
2. Mengontrol akses pengguna dan meningkatkan efisiensi penggunaan sumber daya
3. Menghapus data yang tidak terpakai secara otomatis
4. Menghubungkan perangkat langsung ke internet
5. Memblokir semua lalu lintas tanpa filter

**ANS**: B

###### Apersepsi

Mikrotik memiliki fitur NAT (Network Address Translation) yang memungkinkan pengelolaan alamat IP untuk menghubungkan perangkat internal ke jaringan eksternal secara efisien.

###### Soal

Apa fungsi utama fitur NAT pada Mikrotik?

1. Menghubungkan perangkat langsung ke jaringan publik
2. Mengubah alamat IP internal menjadi alamat IP eksternal untuk lalu lintas keluar
3. Memblokir semua akses dari alamat IP tertentu
4. Mempercepat akses data antar perangkat internal
5. Menghapus log aktivitas pengguna

**ANS**: B

###### Apersepsi

Fitur bandwidth management pada Mikrotik digunakan untuk mengontrol alokasi bandwidth untuk setiap pengguna di jaringan.

###### Soal

Apa langkah pertama dalam mengonfigurasi bandwidth management di Mikrotik?

1. Menghapus pengguna lama dari jaringan
2. Menyusun aturan firewall baru
3. Menentukan queue sederhana untuk membatasi bandwidth pengguna tertentu
4. Mengaktifkan fitur logging otomatis
5. Menambahkan ACL untuk akses pengguna

**ANS**: C

###### Apersepsi

Squid Proxy pada Ubuntu memungkinkan administrator untuk membatasi akses situs tertentu berdasarkan aturan ACL (Access Control List).

###### Soal

Apa tujuan utama dari ACL pada Squid Proxy?

1. Menyimpan data log pengguna secara permanen
2. Membatasi akses ke situs tertentu atau layanan internet tertentu
3. Mempercepat koneksi dengan caching otomatis
4. Menghapus semua ancaman dari jaringan internal
5. Menghubungkan perangkat langsung ke internet

**ANS**: B

###### Apersepsi

Mikrotik memungkinkan konfigurasi firewall yang lebih kompleks dengan fitur mangle untuk menandai lalu lintas data tertentu.

###### Soal

Apa manfaat utama dari fitur mangle pada firewall Mikrotik?

1. Mempercepat lalu lintas data tanpa filter
2. Menandai lalu lintas data untuk pengaturan lanjutan seperti routing atau queue
3. Menghapus log pengguna yang tidak aktif
4. Memblokir semua lalu lintas data secara otomatis
5. Menyimpan log aktivitas dalam jumlah besar

**ANS**: B

###### Apersepsi

Fitur DHCP server pada Mikrotik memudahkan administrator untuk memberikan alamat IP secara otomatis kepada perangkat yang terhubung ke jaringan.

###### Soal

Apa fungsi utama dari DHCP server di Mikrotik?

1. Menghapus alamat IP perangkat lama
2. Memberikan alamat IP secara otomatis kepada perangkat yang terhubung
3. Mengontrol bandwidth perangkat tertentu
4. Memblokir perangkat asing dari jaringan
5. Menghubungkan perangkat langsung ke jaringan publik

**ANS**: B

###### Apersepsi

Proxy eksternal sering digunakan untuk membatasi akses dari jaringan publik ke jaringan internal, memberikan perlindungan tambahan terhadap ancaman.

###### Soal

Apa langkah penting dalam konfigurasi proxy eksternal di Ubuntu menggunakan Squid Proxy?

1. Menyimpan data log pengguna tanpa batas waktu
2. Menambahkan aturan akses dalam file konfigurasi Squid
3. Mengaktifkan NAT secara otomatis
4. Membatasi bandwidth tanpa pengaturan tambahan
5. Menghapus cache pengguna lama

**ANS**: B

###### Apersepsi

Mikrotik memiliki fitur Queue Tree yang memberikan kontrol lebih detail terhadap alokasi bandwidth untuk berbagai layanan atau pengguna.

###### Soal

Apa langkah pertama dalam mengonfigurasi Queue Tree pada Mikrotik?

1. Menentukan target alamat IP atau port yang akan diatur
2. Menghapus log aktivitas lama
3. Menyusun daftar situs yang akan dibatasi
4. Mengaktifkan NAT untuk perangkat lokal
5. Menghubungkan perangkat langsung ke jaringan

**ANS**: A

###### Apersepsi

Log firewall pada Mikrotik dapat memberikan informasi tentang aktivitas jaringan, termasuk serangan yang terdeteksi dan lalu lintas yang diblokir.

###### Soal

Apa tujuan utama dari log firewall pada Mikrotik?

1. Menyimpan data pengguna secara permanen
2. Memonitor aktivitas jaringan dan mendeteksi ancaman
3. Mempercepat koneksi antar perangkat lokal
4. Menghapus ancaman malware secara otomatis
5. Membatasi akses pengguna ke situs tertentu

**ANS**: B

###### Apersepsi

Mengintegrasikan proxy server dengan firewall memberikan lapisan perlindungan tambahan terhadap lalu lintas data yang mencurigakan.

###### Soal

Apa keuntungan utama dari integrasi proxy server dengan firewall?

1. Memblokir semua akses dari alamat IP luar
2. Meningkatkan keamanan dengan menyaring lalu lintas berdasarkan aturan ganda
3. Menghapus semua data log pengguna yang tidak aktif
4. Mempercepat akses internet tanpa konfigurasi tambahan
5. Mengontrol bandwidth perangkat tanpa pengaturan proxy

**ANS**: B

###### Apersepsi

Fitur bridge pada Mikrotik memungkinkan penggabungan beberapa antarmuka jaringan menjadi satu segment jaringan.

###### Soal

Apa fungsi utama dari bridge pada Mikrotik?

1. Menghapus alamat IP perangkat lama
2. Menggabungkan beberapa antarmuka jaringan menjadi satu segmen
3. Mempercepat transfer data antar perangkat di jaringan lokal
4. Membatasi akses pengguna ke jaringan publik
5. Menghubungkan perangkat langsung ke jaringan internet

**ANS**: B

###### Apersepsi

Konfigurasi firewall di Ubuntu menggunakan iptables memungkinkan administrator untuk menetapkan aturan keamanan pada server.

###### Soal

Apa langkah pertama dalam konfigurasi firewall menggunakan iptables?

1. Menambahkan alamat IP pengguna yang diizinkan
2. Menentukan chain untuk aturan yang akan diterapkan
3. Menghapus semua log aktivitas lama
4. Membatasi bandwidth pengguna jaringan lokal
5. Menghubungkan perangkat langsung ke server

**ANS**: B

###### Apersepsi

Mikrotik memungkinkan konfigurasi port forwarding untuk mengarahkan lalu lintas dari port tertentu ke perangkat tertentu di jaringan internal.

###### Soal

Apa manfaat utama dari port forwarding pada Mikrotik?

1. Menghapus data log yang tidak diperlukan
2. Mengarahkan lalu lintas ke perangkat tertentu dalam jaringan internal
3. Memblokir semua akses dari jaringan publik
4. Membatasi bandwidth pengguna di jaringan lokal
5. Menyimpan log aktivitas pengguna tanpa batas waktu

**ANS**: B

###### Apersepsi

Firewall pada Mikrotik memiliki fitur connection tracking yang memungkinkan pelacakan status koneksi data.

###### Soal

Apa tujuan utama dari connection tracking pada firewall Mikrotik?

1. Memblokir semua lalu lintas data dari perangkat tertentu
2. Melacak status koneksi untuk memastikan validitas paket data
3. Menghapus ancaman malware secara otomatis
4. Mengontrol bandwidth untuk perangkat tertentu
5. Menghubungkan perangkat langsung ke jaringan publik

**ANS**: B

###### Apersepsi

Mikrotik memungkinkan konfigurasi VLAN untuk memisahkan segmen jaringan dengan cara yang efisien dan aman.

###### Soal

Apa langkah pertama dalam konfigurasi VLAN pada Mikrotik?

1. Menentukan ID VLAN dan port yang akan digunakan
2. Menghapus semua perangkat lama dari jaringan
3. Mempercepat koneksi antar perangkat di jaringan lokal
4. Membatasi akses pengguna ke internet
5. Menyimpan data log VLAN secara otomatis

**ANS**: A

##### Kunci Jawaban:

Berikut adalah tabel kunci jawaban untuk 50 soal yang telah dibuat:

|  |  |
| --- | --- |
| **Nomor Soal** | **Kunci Jawaban** |
| 1 | B |
| 2 | C |
| 3 | A |
| 4 | D |
| 5 | B |
| 6 | A |
| 7 | C |
| 8 | E |
| 9 | B |
| 10 | D |
| 11 | A |

|  |  |
| --- | --- |
| **Nomor Soal** | **Kunci Jawaban** |
| 12 | B |
| 13 | C |
| 14 | E |
| 15 | A |
| 16 | D |
| 17 | C |
| 18 | B |
| 19 | A |
| 20 | D |
| 21 | B |
| 22 | C |
| 23 | E |
| 24 | D |
| 25 | A |
| 26 | B |
| 27 | C |
| 28 | E |
| 29 | A |
| 30 | D |
| 31 | B |
| 32 | C |
| 33 | A |
| 34 | E |
| 35 | D |
| 36 | C |
| 37 | A |
| 38 | B |
| 39 | C |
| 40 | D |
| 41 | A |
| 42 | B |
| 43 | E |
| 44 | C |
| 45 | D |
| 46 | B |
| 47 | A |
| 48 | E |
| 49 | C |
| 50 | B |

* 1. Penilaian Sikap Profil Pelajar Pancasila

Penilaian sikap adalah bagian penting untuk mengevaluasi aspek nilai-nilai **Profil Pelajar Pancasila**, meliputi: **Mandiri**, **Bergotong Royong**, **Bernalar Kritis**, **Berkebhinekaan Global**, dan **Kreatif**.

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **No** | **Nama Siswa** | **Mandiri** | **Bergotong Royong** | **Bernalar Kritis** | **Berkebhinekaan Global** | **Kreatif** | **Nilai Akhir** |  |
|  |  | 4 | 3 | 4 | 4 | 3 | 18 |  |
| 1 |  |  |  |  |  |  |  |  |
| 2 |  |  |  |  |  |  |  |  |
| 3 |  |  |  |  |  |  |  |  |
| 4 |  |  |  |  |  |  |  |  |
| 5 |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |

* + 1. Rubrik Penilaian Sikap Profil Pelajar Pancasila

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Aspek yang Dinilai** | **Skor 4 (Sangat Baik)** | **Skor 3 (Baik)** | **Skor 2 (Cukup)** | **Skor 1 (Kurang)** |
| **Mandiri** | Selalu aktif, bekerja | Aktif dan mandiri | Kadang-kadang aktif, | Tidak aktif, selalu |
|  | dengan inisiatif tinggi, | dalam menyelesaikan | masih perlu bimbingan | membutuhkan |
|  | dan menyelesaikan tugas dengan sangat | tugas, tetapi terkadang | untuk menyelesaikan tugas. | bantuan untuk menyelesaikan tugas. |
|  | baik. | membutuhkan |  |  |
|  |  | bimbingan. |  |  |
| **Bergotong** | Selalu menghargai | Berkolaborasi dengan | Kadang bekerja sama, | Tidak bekerja sama |
| **Royong** | pendapat, aktif bekerja sama, dan berkontribusi | baik, tetapi kurang konsisten dalam | tetapi sering pasif dalam diskusi | dengan tim dan cenderung tidak |
|  | penuh dalam tim. | membantu tim. | kelompok. | menghargai pendapat |
|  |  |  |  | teman. |
| **Bernalar Kritis** | Menganalisis masalah | Dapat menganalisis | Mampu | Tidak mampu |
|  | dengan sangat baik, mampu memberi solusi | masalah dan memberi solusi sederhana. | mengidentifikasi masalah tetapi | menganalisis masalah dan |
|  | inovatif. |  | kesulitan memberikan | memberikan solusi. |
|  |  |  | solusi yang relevan. |  |
| **Berkebhinekaan** | Selalu menghormati | Menghargai | Mengetahui | Kurang menghargai |
| **Global** | keberagaman, menyadari pentingnya | keberagaman tetapi belum selalu | keberagaman tetapi tidak menunjukkan | keberagaman, sering tidak menunjukkan |
|  | kolaborasi lintas | menunjukkan sikap | sikap menghargai | inklusivitas dalam |
|  | budaya, dan | inklusif dalam diskusi | perspektif lain secara | berkolaborasi. |
|  | menunjukkan | atau kolaborasi. | konsisten. |  |
|  | inklusivitas tinggi. |  |  |  |
| **Kreatif** | Memberikan solusi | Memberikan solusi | Kadang memberikan | Tidak menunjukkan |
|  | inovatif yang di luar | yang baik meskipun | ide baru, tetapi sering | kreativitas atau |
|  | kebiasaan, serta | belum terlalu inovatif. | hanya mengikuti | inovasi, cenderung |
|  | menciptakan  pendekatan baru dalam |  | instruksi. | mengandalkan solusi dari orang lain. |
|  | menyelesaikan tugas. |  |  |  |

* + 1. Skala Penilaian Sikap

|  |  |
| --- | --- |
| **Skor** | **Deskripsi** |
| **16-20** | **Sangat Baik**: Peserta didik sangat aktif, menunjukkan sikap terbaik pada semua aspek. |
| **11-15** | **Baik**: Peserta didik memiliki sikap baik, tetapi masih ada ruang untuk peningkatan. |
| **6-10** | **Cukup**: Peserta didik menunjukkan sikap cukup, tetapi perlu bimbingan lebih lanjut. |
| **1-5** | **Kurang**: Peserta didik perlu perbaikan signifikan dalam sikap dan kerja sama. |

* 1. Penilaian Praktik

Berikut adalah tabel **Lembar Penilaian Praktik** yang dapat digunakan untuk menilai keterampilan peserta didik dalam setiap LKPD dari **LKPD 1 hingga LKPD 18**:

##### Lembar Penilaian Praktik

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Pertemuan / LKPD** | **Kegiatan Praktik** | **Indikator Penilaian** | **Skala**  **Penilaian** | **Skor Maksimal** |
| **LKPD 1** | Pengantar Firewall: Menjelaskan definisi dan fungsi firewall | 1. Memahami konsep dasar firewall | 1-4 | 4 |
|  |  | 2. Menyebutkan jenis-jenis firewall | 1-4 | 4 |
| **LKPD 2** | Arsitektur dan Desain Firewall: Mendesain arsitektur firewall | 1. Menyusun desain firewall yang sesuai dengan kebutuhan jaringan | 1-4 | 4 |
|  |  | 2. Memilih desain yang tepat berdasarkan studi kasus | 1-4 | 4 |
| **LKPD 3** | Packet Filtering dengan Mikrotik: Mengonfigurasi packet filtering | 1. Mengonfigurasi aturan packet filtering sesuai skenario praktikum | 1-4 | 4 |
|  |  | 2. Menguji dan memverifikasi konfigurasi yang telah dibuat | 1-4 | 4 |
| **LKPD 4** | Konfigurasi dan Pengelolaan Firewall: Mengonfigurasi aturan firewall | 1. Mengatur aturan firewall dasar pada Mikrotik | 1-4 | 4 |
|  |  | 2. Mengelola kebijakan firewall dengan benar | 1-4 | 4 |
| **LKPD 5** | Monitor dan Log Aktivitas Firewall: Mengaktifkan dan memantau log firewall | 1. Mengaktifkan logging pada Mikrotik | 1-4 | 4 |
|  |  | 2. Menganalisis log aktivitas untuk mendeteksi ancaman | 1-4 | 4 |
| **LKPD 6** | Implementasi Firewall dalam Jaringan: Mengimplementasikan firewall | 1. Mengonfigurasi firewall sesuai dengan kebutuhan jaringan  perusahaan | 1-4 | 4 |
|  |  | 2. Menguji kebijakan firewall pada jaringan perusahaan | 1-4 | 4 |
| **LKPD 7** | Tantangan dan Tren Terbaru dalam Firewall: Memahami NGFW | 1. Menerapkan pengetahuan tentang NGFW dan kelebihannya | 1-4 | 4 |
|  |  | 2. Mengintegrasikan NGFW dengan IDS/IPS | 1-4 | 4 |
| **LKPD 8** | Pengantar Proxy Server: Mengonfigurasi Proxy Server | 1. Memahami fungsi dan jenis- jenis proxy server | 1-4 | 4 |
|  |  | 2. Mengonfigurasi proxy server sesuai skenario jaringan | 1-4 | 4 |
| **LKPD 9** | Proxy Internal dengan Mikrotik: Mengonfigurasi Proxy Internal | 1. Mengonfigurasi proxy internal pada Mikrotik | 1-4 | 4 |
|  |  | 2. Membatasi akses menggunakan proxy internal Mikrotik | 1-4 | 4 |
| **LKPD 10** | Proxy Eksternal dengan Ubuntu: Mengonfigurasi Proxy Server Eksternal | 1. Menginstal dan mengonfigurasi Squid Proxy pada Ubuntu | 1-4 | 4 |
|  |  | 2. Mengelola kebijakan akses eksternal melalui proxy Ubuntu | 1-4 | 4 |
| **LKPD 11** | Pengaturan Kebijakan Proxy Server: Membuat Kebijakan Akses | 1. Mengatur kebijakan proxy berdasarkan waktu dan jenis | 1-4 | 4 |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Pertemuan / LKPD** | **Kegiatan Praktik** | **Indikator Penilaian** | **Skala**  **Penilaian** | **Skor Maksimal** |
|  |  | konten |  |  |
|  |  | 2. Mengonfigurasi proxy untuk membatasi akses sesuai kebijakan | 1-4 | 4 |
| **LKPD 12** | Monitoring Lalu Lintas Jaringan dengan Mikrotik: Menggunakan fitur monitoring | 1. Menggunakan fitur monitoring Mikrotik untuk memantau lalu lintas | 1-4 | 4 |
|  |  | 2. Mendeteksi aktivitas mencurigakan melalui fitur monitoring | 1-4 | 4 |
| **LKPD 13** | Fitur-Fitur Keamanan pada Mikrotik: Mengonfigurasi fitur keamanan | 1. Mengonfigurasi firewall, NAT, dan fitur keamanan Mikrotik | 1-4 | 4 |
|  |  | 2. Mengelola fitur logging dan filtering pada Mikrotik | 1-4 | 4 |
| **LKPD 14** | Analisis dan Optimalisasi Keamanan Jaringan: Menggunakan data monitoring | 1. Menganalisis data hasil monitoring untuk deteksi ancaman | 1-4 | 4 |
|  |  | 2. Mengoptimalkan kebijakan keamanan berdasarkan analisis data | 1-4 | 4 |
| **LKPD 15** | Pengaturan Kebijakan Keamanan pada Mikrotik: Menyusun Kebijakan  Keamanan | 1. Menyusun kebijakan keamanan berdasarkan analisis | 1-4 | 4 |
|  |  | 2. Mengonfigurasi kebijakan di Mikrotik untuk melindungi jaringan | 1-4 | 4 |
| **LKPD 16** | Praktik Deteksi dan Mitigasi Ancaman dengan Mikrotik: Mendeteksi dan Mengatasi Ancaman | 1. Mendeteksi ancaman pada  jaringan Mikrotik menggunakan teknik deteksi | 1-4 | 4 |
|  |  | 2. Mengonfigurasi mitigasi  ancaman menggunakan aturan firewall | 1-4 | 4 |
| **LKPD 17** | Review dan Ujian Praktik Firewall &  Proxy: Review materi dan ujian praktik | 1. Menyelesaikan ujian praktik dengan benar | 1-4 | 4 |
|  |  | 2. Memahami konsep dan  penerapan firewall dan proxy dalam jaringan | 1-4 | 4 |
| **LKPD 18** | Refleksi dan Kesimpulan Semester: Diskusi dan refleksi materi | 1. Merenungkan dan menyimpulkan materi  pembelajaran yang telah dipelajari | 1-4 | 4 |
|  |  | 2. Memberikan rekomendasi untuk pengelolaan keamanan jaringan di masa depan | 1-4 | 4 |

Keterangan:

**Skala Penilaian**: 1-4 (1: Kurang, 2: Cukup, 3: Baik, 4: Sangat Baik)

**Skor Maksimal**: Setiap pertemuan diberi skor maksimal 4 poin untuk setiap indikator. Total skor untuk setiap LKPD adalah 8, karena terdiri dari dua indikator yang masing-masing dinilai dari 1 hingga 4.

###### Instruksi Penilaian:

**Skor 4**: Peserta didik menunjukkan keterampilan yang sangat baik dalam konfigurasi, pemahaman, dan implementasi materi praktikum.

**Skor 3**: Peserta didik menunjukkan keterampilan yang baik dengan sedikit kekurangan atau kesalahan minor.

**Skor 2**: Peserta didik menunjukkan keterampilan yang cukup tetapi membutuhkan perbaikan dalam beberapa area. **Skor 1**: Peserta didik menunjukkan keterampilan yang kurang, dengan banyak kesalahan atau tidak mampu menyelesaikan tugas dengan benar.

#### Bahan Bacaan Pendidik dan Peserta Didik

1. Pengantar Firewall

###### Definisi dan Fungsi Firewall:

Firewall adalah sistem pengendalian lalu lintas jaringan yang berfungsi untuk mengatur, mengizinkan, atau memblokir paket data berdasarkan serangkaian aturan keamanan yang telah ditentukan. Fungsi utamanya adalah untuk melindungi jaringan internal dari ancaman yang berasal dari luar (misalnya, hacker, malware, dan virus), serta untuk mengatur komunikasi antar perangkat di dalam jaringan.

###### Jenis-Jenis Firewall:

* 1. **Firewall Hardware**: Biasanya berupa perangkat fisik yang ditempatkan di antara jaringan internal dan eksternal untuk mengontrol aliran data. Kelebihannya adalah lebih aman dan dapat menangani lalu lintas data lebih banyak.
  2. **Firewall Software**: Merupakan perangkat lunak yang dipasang pada komputer atau server untuk memfilter lalu lintas jaringan. Mudah dipasang dan digunakan, tetapi seringkali lebih lambat dibandingkan firewall hardware.
  3. **Stateful Firewall**: Firewall yang melacak status koneksi yang sedang berlangsung, sehingga bisa memeriksa paket data dengan lebih cerdas berdasarkan status koneksi.
  4. **Stateless Firewall**: Firewall yang hanya memeriksa data berdasarkan aturan yang ada tanpa mempertimbangkan status koneksi. Lebih cepat, tetapi kurang canggih dibandingkan dengan stateful firewall.

###### Referensi:

**"Network Security Essentials"** oleh William Stallings

**"Firewalls and Internet Security: Repelling the Wily Hacker"** oleh William R. Cheswick dan Steven M. Bellovin

**MikroTik Official Documentation**: [www.mikrotik.com](https://www.mikrotik.com/)

1. Arsitektur dan Desain Firewall

###### Desain Arsitektur Firewall:

Firewall dapat diterapkan dalam berbagai arsitektur jaringan. Beberapa desain yang umum digunakan antara lain:

* 1. **Perimeter Firewall**: Firewall yang mengatur lalu lintas data di perimeter atau batasan jaringan internal dan eksternal.
  2. **Dual-Homed Firewall**: Firewall yang memiliki dua interface (antarmuka), satu untuk koneksi internal dan satu untuk koneksi eksternal.
  3. **DMZ (Demilitarized Zone)**: Jaringan terpisah yang menghubungkan jaringan internal dan eksternal, digunakan untuk melindungi server yang diakses dari luar seperti web server, email server, dan FTP server.

###### Referensi:

**"Computer Security: Principles and Practice"** oleh William Stallings dan Lawrie Brown

**"The Art of Network Security Monitoring"** oleh Eric Cole

1. Packet Filtering dan Mikrotik

###### Packet Filtering pada Mikrotik:

Packet filtering adalah teknik yang digunakan untuk memfilter lalu lintas data berdasarkan aturan yang ditetapkan. Pada Mikrotik, Anda dapat membuat aturan packet filtering yang mengatur akses berdasarkan berbagai parameter seperti alamat IP, port, dan protokol.

Contoh aturan packet filtering di Mikrotik:

**Drop traffic** dari alamat IP tertentu (misalnya, 192.168.1.10)

**Allow traffic** untuk port tertentu (misalnya, port 80 untuk HTTP)

###### Referensi:

**MikroTik RouterOS Documentation**: [www.mikrotik.com](https://www.mikrotik.com/)

1. Pengelolaan Kebijakan Firewall

###### Mengonfigurasi Kebijakan Akses pada Firewall:

Firewall dapat digunakan untuk mengelola akses ke jaringan dengan menggunakan aturan yang membatasi jenis komunikasi yang dapat dilakukan oleh perangkat di jaringan tersebut. Kebijakan ini dapat disusun untuk:

Mengizinkan akses hanya pada jam tertentu (misalnya, akses administratif hanya boleh pada jam kerja). Memblokir akses ke aplikasi tertentu (misalnya, membatasi akses ke situs sosial media atau aplikasi game).

###### Referensi:

**"Network Security Bible"** oleh Eric Cole

**"Firewall Fundamentals"** oleh Wes Noonan

1. Pengantar Proxy Server

###### Definisi dan Fungsi Proxy Server:

Proxy server adalah sistem yang berfungsi sebagai perantara antara pengguna dan internet. Dengan proxy, pengguna dapat mengakses internet tanpa langsung terhubung ke server tujuan. Fungsi utama proxy server adalah untuk menyaring konten, mempercepat akses melalui caching, dan menjaga privasi pengguna dengan menyembunyikan alamat IP asli.

###### Jenis-Jenis Proxy:

* 1. **Forward Proxy**: Menghubungkan pengguna ke server yang diinginkan dan menyembunyikan alamat IP pengguna.
  2. **Reverse Proxy**: Menghubungkan pengguna ke server web internal, sering digunakan untuk load balancing atau menyembunyikan server internal dari publik.
  3. **Transparent Proxy**: Proxy yang tidak memerlukan konfigurasi pada perangkat pengguna dan dapat digunakan untuk caching atau pembatasan konten.

###### Referensi:

**"Web Proxy Servers"** oleh Tarek S. S. El-Sayed

**"Proxy and Web Caching"** oleh K. K. Ramakrishnan dan K. L. Pham

**Squid Proxy Official Documentation**: [www.squid-cache.org](http://www.squid-cache.org/)

1. Pengelolaan Proxy Server di Mikrotik

###### Konfigurasi Proxy Internal pada Mikrotik:

Proxy internal pada Mikrotik digunakan untuk menyaring dan mempercepat akses internet bagi pengguna di jaringan internal. Proxy ini bisa digunakan untuk mengontrol akses ke situs tertentu serta menyimpan cache situs yang sering diakses untuk mempercepat waktu muat halaman.

Contoh konfigurasi proxy internal:

Mengaktifkan fitur **web proxy**.

Menambahkan aturan untuk **memblokir akses ke domain tertentu**.

###### Referensi:

**MikroTik RouterOS Documentation**: [www.mikrotik.com](https://www.mikrotik.com/)

1. Proxy Server Eksternal dan Ubuntu

###### Instalasi dan Konfigurasi Squid Proxy di Ubuntu:

Squid adalah salah satu aplikasi proxy server yang paling banyak digunakan, terutama untuk proxy eksternal. Squid dapat diinstal di Ubuntu untuk mengelola akses internet dari pengguna internal ke luar jaringan.

Langkah-langkah dasar konfigurasi Squid Proxy:

* 1. Instal Squid Proxy dengan perintah:

sudo apt install squid

* 1. Konfigurasikan file **squid.conf** untuk mengatur akses, misalnya dengan membatasi akses ke situs tertentu atau mempercepat akses melalui cache.

###### Referensi:

**Squid Proxy Documentation**: [www.squid-cache.org](http://www.squid-cache.org/)

1. Kebijakan Penggunaan Proxy

###### Menerapkan Kebijakan Akses pada Proxy Server:

Proxy server dapat digunakan untuk mengatur kebijakan penggunaan internet di organisasi atau sekolah. Kebijakan tersebut bisa meliputi:

Pembatasan waktu akses ke internet.

Pembatasan akses ke konten tertentu, seperti situs media sosial atau situs dewasa. Pengaturan akses hanya pada perangkat tertentu yang sudah terdaftar.

###### Referensi:

**"Proxy Server: How to Build a Proxy Server"** oleh Steve Jansen

Sumber Referensi Umum untuk Firewall dan Proxy:

**"Network Security: A Beginner’s Guide"** oleh Eric Maiwald

**"Firewall and VPN Configuration Handbook"** oleh Syngress Publishing

**"The Web Application Hacker's Handbook"** oleh Dafydd Stuttard dan Marcus Pinto

**MikroTik RouterOS User Manual**: [www.mikrotik.com](https://www.mikrotik.com/)

#### Pengayaan dan Remedial

Berikut adalah contoh **Pengayaan** dan **Remedial** yang dapat Anda terapkan berdasarkan materi dalam modul ajar yang Anda buat tentang **Firewall** dan **Proxy**:

* 1. Pengayaan

Pengayaan bertujuan untuk memperdalam pemahaman bagi peserta didik yang telah menguasai materi dan ingin mempelajari topik yang lebih kompleks.

##### Pengayaan untuk Firewall

**Topik**: *Next-Generation Firewall (NGFW)*

**Deskripsi**: Untuk peserta didik yang telah memahami konsep dasar tentang firewall, mereka dapat melanjutkan untuk mempelajari **Next-Generation Firewall (NGFW)** yang menawarkan fitur-fitur tambahan seperti inspeksi mendalam (Deep Packet Inspection), pencegahan intrusi (IPS), dan deteksi ancaman berbasis aplikasi.

###### Kegiatan:

Pelajari konsep NGFW dan bagaimana membedakannya dengan firewall tradisional. Praktikkan penerapan NGFW di Mikrotik atau perangkat sejenis (jika tersedia).

Diskusi tentang bagaimana NGFW dapat diintegrasikan dengan sistem IDS/IPS dalam jaringan perusahaan.

**Proyek Tugas**: Buatlah proposal untuk penerapan NGFW di sebuah organisasi atau perusahaan fiktif, lengkap dengan justifikasi teknis dan keamanan.

###### Bahan Bacaan:

Artikel tentang NGFW di [Cisco](https://www.cisco.com/c/en/us/products/security/next-generation-firewall/index.html)

Buku *"Next Generation Firewall: The Complete Guide"* oleh Michael D. Bruns

##### Pengayaan untuk Proxy

**Topik**: *Proxy Server dan Teknologi Anonimitas (Tor, VPN)*

**Deskripsi**: Setelah peserta didik memahami dasar-dasar proxy server, mereka bisa melanjutkan untuk mempelajari

**Proxy Server yang digunakan dalam teknologi anonim**, seperti **Tor** dan **VPN**. **Kegiatan**:

Pelajari perbedaan antara **Tor (The Onion Router)**, **VPN (Virtual Private Network)**, dan **Proxy** dalam hal privasi dan keamanan.

Praktikkan penggunaan Tor atau VPN dalam mengakses internet dan bandingkan dengan penggunaan proxy biasa.

**Proyek Tugas**: Buatlah laporan tentang cara kerja Tor dan VPN dalam menjaga anonimitas online serta penerapannya dalam dunia nyata.

###### Bahan Bacaan:

[The Tor Project - https://www.torproject.org/](https://www.torproject.org/) Buku *"VPNs and Proxy Servers"*

* 1. Remedial

Remedial bertujuan untuk memberikan pemahaman lebih lanjut bagi peserta didik yang mengalami kesulitan dalam memahami materi.

##### Remedial untuk Firewall

**Topik**: *Dasar-dasar Firewall dan Jenis-jenis Firewall*

**Deskripsi**: Jika peserta didik kesulitan memahami konsep dasar firewall atau jenis-jenis firewall, mereka bisa diberikan remedial berupa penjelasan lebih sederhana dan latihan dasar untuk memperkuat pemahaman.

###### Kegiatan:

**Pengulangan Materi**: Ulas kembali pengertian dasar firewall dan jenis-jenis firewall (hardware, software, stateful, stateless). Gunakan analogi untuk mempermudah pemahaman, misalnya dengan menggambarkan firewall seperti penjaga pintu yang memilih siapa yang bisa masuk atau keluar.

**Latihan Praktik**: Lakukan sesi praktik dengan cara mengonfigurasi firewall sederhana di Mikrotik atau menggunakan **Firewall Builder** untuk memperkenalkan dasar konfigurasi dan cara kerjanya.

**Tugas**: Buatlah sebuah diagram alur yang menjelaskan bagaimana **stateful** dan **stateless firewall** bekerja dan berbeda.

###### Bahan Bacaan:

*"Firewall For Dummies"* oleh Jonathan S. R.

Artikel singkat mengenai firewall dasar: [Firewall Basics](https://www.webopedia.com/definitions/firewall/)

* + 1. Remedial untuk Proxy

**Topik**: *Pengertian dan Penggunaan Proxy Server*

**Deskripsi**: Untuk peserta didik yang kesulitan memahami konsep proxy server, bisa diberikan remedial dengan fokus pada pengertian dasar, fungsi, dan cara kerjanya.

###### Kegiatan:

**Penjelasan Ulang**: Berikan penjelasan lebih rinci tentang bagaimana **proxy server** berfungsi untuk menghubungkan pengguna dengan internet dan bagaimana proxy menyaring permintaan dan respons. Gunakan contoh praktis, seperti bagaimana proxy dapat menyaring akses ke situs-situs tertentu di jaringan sekolah.

**Latihan Praktik**: Lakukan konfigurasi proxy di Mikrotik dengan pengaturan sederhana untuk membatasi akses ke situs tertentu (misalnya, blokir akses ke situs media sosial).

**Tugas**: Buatlah laporan yang menjelaskan bagaimana **proxy server** dapat digunakan di organisasi untuk mengontrol akses internet dan melindungi data.

###### Bahan Bacaan:

Artikel: *"What is Proxy Server and How Does it Work?"* dari [Tech Terms](https://www.techterms.com/definition/proxyserver) Buku *"Proxy Servers and Web Caching"*

* 1. Aktivitas Pengayaan dan Remedial:

###### Sumber Materi:

**Artikel, Video, dan Modul Pembelajaran**: Artikel tentang firewall dan proxy yang dapat ditemukan di situs-situs seperti [Cisco](https://www.cisco.com/), [TechTarget](https://www.techtarget.com/), dan [Medium](https://medium.com/).

**Perangkat Mikrotik**: Dapat digunakan untuk praktik konfigurasinya (jika sekolah memiliki perangkat Mikrotik).

**Sumber Tambahan**: Platform pembelajaran daring yang menyediakan kursus tentang keamanan jaringan seperti

**Udemy** atau **Coursera**.

###### Metode Penilaian:

**Ujian Kuis/Soal Pilihan Ganda** untuk mengukur pemahaman dasar.

**Praktik Langsung** untuk menguji keterampilan peserta didik dalam konfigurasi firewall dan proxy.

**Proyek Tugas**: Memberikan studi kasus atau tugas proyek untuk memperdalam penerapan konsep yang dipelajari.

* 1. Tindak Lanjut Pengayaan dan Remedial**:**

###### Pengayaan:

**Eksplorasi lebih dalam tentang NGFW, IDS/IPS, Tor, dan VPN** untuk peserta didik yang tertarik dalam memperluas pengetahuan mereka tentang keamanan jaringan lebih lanjut.

**Tantangan Konfigurasi**: Setiap peserta didik diberi tantangan konfigurasi firewall atau proxy dengan pengaturan yang lebih kompleks dan lebih banyak variabel.

###### Remedial:

**Pendekatan Visual**: Gunakan diagram, video, dan grafik untuk menggambarkan konsep firewall dan proxy lebih mudah dipahami.

**Pendampingan Individu**: Berikan bimbingan langsung kepada peserta didik yang kesulitan, termasuk sesi tanya jawab dan simulasi pengaturan firewall dan proxy pada perangkat jaringan virtual atau fisik.

Dengan adanya **Pengayaan** dan **Remedial** ini, Anda dapat memberikan kesempatan kepada peserta didik yang lebih cepat dalam menguasai materi untuk mengeksplorasi lebih jauh, sementara peserta didik yang kesulitan dapat diberikan bantuan agar bisa mengikuti materi dengan lebih baik.

#### Glosarium

###### Firewall:

Sebuah sistem keamanan jaringan yang berfungsi untuk memantau dan mengendalikan lalu lintas data yang masuk dan keluar dari jaringan. Firewall memfilter paket data berdasarkan aturan yang telah ditentukan, untuk mencegah akses yang tidak sah dan melindungi jaringan dari potensi serangan.

###### Proxy Server:

Server yang bertindak sebagai perantara antara pengguna dan server lainnya di internet. Proxy server dapat menyaring konten internet yang diakses pengguna, mengelola koneksi, serta meningkatkan keamanan dan kinerja dengan caching data dan membatasi akses ke situs tertentu.

###### VPN (Virtual Private Network):

Teknologi yang memungkinkan koneksi aman melalui internet dengan membuat saluran komunikasi terenkripsi, yang melindungi data saat dikirim antara perangkat pengguna dan server tujuan, seperti saat bekerja di jaringan publik.

###### DDoS (Distributed Denial of Service):

Sebuah jenis serangan siber yang melibatkan pengiriman trafik jaringan yang sangat tinggi ke sebuah server atau layanan agar menjadi tidak tersedia bagi pengguna yang sah. DDoS biasanya dilakukan dengan mengendalikan sejumlah besar perangkat yang terinfeksi (botnet) untuk menyerang server target.

###### Port Scanning:

Teknik yang digunakan untuk menemukan port terbuka pada perangkat jaringan yang dapat dieksploitasi oleh pihak yang tidak sah. Port scanning digunakan oleh penyerang untuk mencari celah keamanan yang dapat dimanfaatkan untuk menyusup ke dalam jaringan.

###### IDS (Intrusion Detection System):

Sistem yang digunakan untuk mendeteksi aktivitas mencurigakan atau potensi ancaman di jaringan dengan memonitor aliran data dan mencatat pola yang menunjukkan kemungkinan adanya serangan.

###### IPS (Intrusion Prevention System):

Sistem yang lebih lanjut daripada IDS, di mana ia tidak hanya mendeteksi potensi ancaman tetapi juga **menghentikan serangan** sebelum masuk ke dalam jaringan dengan memblokir paket yang mencurigakan.

###### Stateful Firewall:

Jenis firewall yang tidak hanya memfilter paket data berdasarkan aturan yang telah ditentukan, tetapi juga memonitor status koneksi yang aktif dan memastikan bahwa setiap paket yang dikirim adalah bagian dari koneksi yang sah.

###### Stateless Firewall:

Jenis firewall yang lebih sederhana, yang hanya memfilter paket data berdasarkan aturan yang telah ditentukan tanpa memperhatikan status koneksi yang aktif. Biasanya digunakan untuk pengaturan yang lebih dasar dan tidak memerlukan analisis mendalam.

###### Least Privilege Principle:

Prinsip keamanan yang menyatakan bahwa setiap pengguna atau sistem hanya diberikan hak akses minimum yang

diperlukan untuk melaksanakan tugasnya. Prinsip ini digunakan untuk membatasi potensi kerusakan yang dapat terjadi jika akun pengguna atau sistem tersebut disusupi.

###### ACL (Access Control List):

Daftar aturan yang digunakan untuk menentukan siapa yang dapat mengakses sumber daya tertentu dalam jaringan atau sistem. ACL sering digunakan pada firewall dan router untuk mengontrol akses berdasarkan alamat IP, port, atau protokol.

###### Encryption:

Proses mengubah data asli menjadi format yang tidak dapat dibaca (ciphertext) menggunakan algoritma tertentu, untuk mencegah pihak yang tidak berwenang mengakses informasi tersebut.

###### Packet Filtering:

Teknik di firewall yang memeriksa data yang masuk atau keluar dari jaringan berdasarkan aturan yang telah ditetapkan, seperti alamat IP pengirim, port tujuan, atau protokol yang digunakan.

###### VPN Tunnel:

Terowongan enkripsi yang dibuat oleh VPN untuk mengamankan aliran data antara pengguna dan server. Data yang melewati tunnel ini dilindungi dengan enkripsi yang membuatnya aman dari penyadapan atau intersepsi.

#### Daftar Pustaka

1. **Fitzgerald, J., & Dennis, A. (2017)**. *Business Data Communications and Networking*. 13th Edition. Wiley.

Buku ini memberikan pemahaman yang lebih dalam mengenai konsep dasar jaringan komputer, termasuk topologi jaringan, protokol, dan cara mengelola keamanan jaringan.

1. **Lazarinis, F. (2016)**. *Network Security Essentials*. 6th Edition. Pearson Education.

Buku ini membahas tentang dasar-dasar keamanan jaringan, termasuk firewall, VPN, dan teknik mitigasi ancaman seperti deteksi DDoS dan port scanning.

1. **Mikrotik Documentation**. *Mikrotik RouterOS* [https://wiki.mikrotik.com](https://wiki.mikrotik.com/).

Sumber resmi dokumentasi Mikrotik untuk konfigurasi perangkat jaringan, termasuk penggunaan firewall, VPN, dan fitur keamanan lainnya.

1. **Squid Proxy Documentation**. *Squid Proxy Server* [https://wiki.squid-cache.org](https://wiki.squid-cache.org/).

Dokumentasi resmi mengenai penggunaan Squid Proxy, cara instalasi, serta konfigurasi untuk pengelolaan akses internet yang aman.

1. **Perrin, L. (2018)**. *The Basics of VPNs*. [https://www.techradar.com](https://www.techradar.com/).

Artikel ini memberikan penjelasan dasar mengenai VPN, manfaatnya, serta bagaimana VPN bekerja untuk mengamankan data dan melindungi privasi.

1. **Internet Security Threat Report 2020**. Symantec. [https://www.broadcom.com](https://www.broadcom.com/).

Laporan tahunan yang memberikan wawasan tentang tren ancaman keamanan jaringan global, termasuk analisis serangan DDoS dan taktik mitigasi.