Table of Contents

[1. Identitas dan Informasi Umum 4](#_Toc182601191)

[2. Profil Pelajar Pancasila 4](#_Toc182601192)

[Indikator: 4](#_Toc182601193)

[Indikator: 5](#_Toc182601194)

[3. Sarana dan Prasarana 6](#_Toc182601195)

[Spesifikasi Minimal: 6](#_Toc182601196)

[Perangkat Jaringan: 6](#_Toc182601197)

[Fasilitas Penunjang Lainnya: 6](#_Toc182601198)

[4. Target Peserta Didik 6](#_Toc182601199)

[1. Peserta Didik Reguler/Tipikal: 6](#_Toc182601200)

[2. Peserta Didik dengan Kesulitan Belajar: 6](#_Toc182601201)

[3. Peserta Didik dengan Pencapaian Tinggi: 6](#_Toc182601202)

[Pendekatan Pembelajaran yang Terintegrasi: 6](#_Toc182601203)

[5. Model Pembelajaran: Keamanan Jaringan 6](#_Toc182601204)

[a. Model Pembelajaran: Blended Learning (Pembelajaran Campuran) 6](#_Toc182601205)

[Sesi Tatap Muka (Offline): 6](#_Toc182601206)

[Sesi Online (Online Learning): 6](#_Toc182601207)

[Keuntungan Blended Learning: 6](#_Toc182601208)

[b. Model Pembelajaran: Problem-Based Learning (PBL) 6](#_Toc182601209)

[Fase 1: Identifikasi Masalah 6](#_Toc182601210)

[Fase 2: Penyelesaian Masalah 6](#_Toc182601211)

[Fase 3: Presentasi Solusi 6](#_Toc182601212)

[Keuntungan PBL: 6](#_Toc182601213)

[c. Model Pembelajaran: Project-Based Learning (PjBL) 6](#_Toc182601214)

[Fase 1: Perencanaan Proyek 6](#_Toc182601215)

[Fase 2: Pelaksanaan Proyek 6](#_Toc182601216)

[Fase 3: Evaluasi dan Presentasi Proyek 6](#_Toc182601217)

[Keuntungan PjBL: 7](#_Toc182601218)

[d. Model Pembelajaran: Direct Instruction (Instruksi Langsung) 7](#_Toc182601219)

[Fase 1: Penjelasan Teori 7](#_Toc182601220)

[Fase 2: Demonstrasi Praktik 7](#_Toc182601221)

[Fase 3: Latihan Mandiri 7](#_Toc182601222)

[Keuntungan Direct Instruction: 7](#_Toc182601223)

[6. Pemahaman Bermakna 7](#_Toc182601224)

[Pemahaman Bermakna dalam Pembelajaran Keamanan Jaringan 7](#_Toc182601225)

[1. Keterkaitan dengan Dunia Nyata: 8](#_Toc182601226)

[2. Penerapan Pengetahuan pada Masalah Praktis: 8](#_Toc182601227)

[3. Pengembangan Keterampilan Berpikir Kritis dan Analitis: 8](#_Toc182601228)

[4. Kemampuan Beradaptasi dengan Situasi yang Berubah: 8](#_Toc182601229)

[5. Keterlibatan Aktif dalam Proses Pembelajaran: 8](#_Toc182601230)

[Contoh Pemahaman Bermakna pada Materi Keamanan Jaringan**:** 8](#_Toc182601231)

[1. Firewall: 8](#_Toc182601232)

[2. Proxy Server: 8](#_Toc182601233)

[mencegah akses ke situs berbahaya atau mengatur penggunaan internet di organisasi. 8](#_Toc182601234)

[4. Deteksi dan Mitigasi Ancaman: 8](#_Toc182601235)

[7. Pertanyaan Pemantik 9](#_Toc182601236)

[6. Tentang Firewall: 9](#_Toc182601237)

[7. Tentang Proxy Server: 9](#_Toc182601238)

[8. Tentang VPN: 9](#_Toc182601239)

[9. Tentang Deteksi dan Mitigasi Ancaman: 9](#_Toc182601240)

[10. Tentang Kebijakan Keamanan Jaringan: 9](#_Toc182601241)

[Tujuan Penggunaan Pertanyaan Pemantik**:** 9](#_Toc182601242)

[8. Kompetensi Inti 10](#_Toc182601243)

[Pertemuan Pertama: Pengantar Firewall 11](#_Toc182601244)

[3. Bahan Bacaan Pendidik dan Peserta Didik: 12](#_Toc182601245)

[Pertemuan Kedua: Arsitektur dan Desain Firewall 13](#_Toc182601246)

[3. Bahan Bacaan Pendidik dan Peserta Didik: 14](#_Toc182601247)

[Pertemuan Ketiga: Packet Filtering dengan Mikrotik 14](#_Toc182601248)

[3. Bahan Bacaan Pendidik dan Peserta Didik: 16](#_Toc182601249)

[Pertemuan Keempat: Konfigurasi dan Pengelolaan Firewall 16](#_Toc182601250)

[3. Bahan Bacaan Pendidik dan Peserta Didik: 18](#_Toc182601251)

[Pertemuan Kelima: Monitor dan Log Aktivitas Firewall 18](#_Toc182601252)

[3. Bahan Bacaan Pendidik dan Peserta Didik: 19](#_Toc182601253)

[Pertemuan Keenam: Implementasi Firewall dalam Jaringan 20](#_Toc182601254)

[3. Bahan Bacaan Pendidik dan Peserta Didik: 21](#_Toc182601255)

[Pertemuan Ketujuh: Tantangan dan Tren Terbaru dalam Firewall 21](#_Toc182601256)

[3. Bahan Bacaan Pendidik dan Peserta Didik: 23](#_Toc182601257)

[Pertemuan Kedelapan: Pengantar Proxy Server 23](#_Toc182601258)

[3. Bahan Bacaan Pendidik dan Peserta Didik: 25](#_Toc182601259)

[Pertemuan Kesembilan: Proxy Internal dengan Mikrotik 25](#_Toc182601260)

[3. Bahan Bacaan Pendidik dan Peserta Didik: 26](#_Toc182601261)

[Pertemuan Kesepuluh: Proxy Eksternal dengan Ubuntu 27](#_Toc182601262)

[3. Bahan Bacaan Pendidik dan Peserta Didik: 28](#_Toc182601263)

[Pertemuan Kesebelas: Pengaturan Kebijakan Proxy Server 29](#_Toc182601264)

[3. Bahan Bacaan Pendidik dan Peserta Didik: 30](#_Toc182601265)

[Pertemuan Keduabelas: Monitoring Lalu Lintas Jaringan dengan Mikrotik 30](#_Toc182601266)

[3. Bahan Bacaan Pendidik dan Peserta Didik: 32](#_Toc182601267)

[Pertemuan Ketiga belas: Fitur-Fitur Keamanan pada Mikrotik 32](#_Toc182601268)

[3. Bahan Bacaan Pendidik dan Peserta Didik: 34](#_Toc182601269)

[Pertemuan Keempat belas: Analisis dan Optimalisasi Keamanan Jaringan 34](#_Toc182601270)

[3. Bahan Bacaan Pendidik dan Peserta Didik: 35](#_Toc182601271)

[Pertemuan Kelima belas: Pengaturan Kebijakan Keamanan pada Mikrotik 36](#_Toc182601272)

[3. Bahan Bacaan Pendidik dan Peserta Didik: 37](#_Toc182601273)

[Pertemuan Keenam belas: Praktik Deteksi dan Mitigasi Ancaman dengan Mikrotik 38](#_Toc182601274)

[3. Bahan Bacaan Pendidik dan Peserta Didik: 39](#_Toc182601275)

[Pertemuan Ketujuh belas: Review dan Ujian Praktek Firewall & Proxy 40](#_Toc182601276)

[3. Bahan Bacaan Pendidik dan Peserta Didik: 41](#_Toc182601277)

[Pertemuan Kedelapan belas: Refleksi dan Kesimpulan Semester 41](#_Toc182601278)

[3. Bahan Bacaan Pendidik dan Peserta Didik: 43](#_Toc182601279)

[9. INSTRUMEN PENILAIAN 43](#_Toc182601280)

[Kunci Jawaban dan Skor: 44](#_Toc182601281)

[Rubrik Penilaian: 45](#_Toc182601282)

[Deskripsi Penilaian: 45](#_Toc182601283)

[Skala Penilaian: 46](#_Toc182601284)

[Aspek yang Dinilai dalam Penilaian Sikap: 47](#_Toc182601285)

[1. Sikap Terhadap Pembelajaran 47](#_Toc182601286)

[2. Sikap Terhadap Kerja Sama 47](#_Toc182601287)

[3. Sikap Terhadap Tanggung Jawab 47](#_Toc182601288)

[4. Sikap Terhadap Keamanan Data dan Privasi 47](#_Toc182601289)

[5. Sikap Terhadap Penerapan Prinsip Etika 47](#_Toc182601290)

[Penilaian Nilai Akhir**:** 49](#_Toc182601291)

[Rencana Tindak Lanjut**:** 50](#_Toc182601292)

[Rencana Tindak Lanjut Penilaian Keamanan Jaringan 50](#_Toc182601293)

[1. Penilaian Pengetahuan (Asesmen Sumatif) 50](#_Toc182601294)

[Skor 86-100% (Sangat Baik): Tindak Lanjut: 50](#_Toc182601295)

[Skor 66-85% (Baik): Tindak Lanjut: 50](#_Toc182601296)

[Skor 41-65% (Cukup): Tindak Lanjut: 50](#_Toc182601297)

[Skor 0-40% (Kurang): Tindak Lanjut: 50](#_Toc182601298)

[2. Penilaian Keterampilan (Praktek Firewall & Proxy) 51](#_Toc182601299)

[Skor 86-100% (Sangat Baik): Tindak Lanjut: 51](#_Toc182601300)

[Skor 66-85% (Baik): Tindak Lanjut: 51](#_Toc182601301)

[Skor 41-65% (Cukup): Tindak Lanjut: 51](#_Toc182601302)

[deteksi ancaman sederhana. 51](#_Toc182601303)

[Skor 0-40% (Kurang): Tindak Lanjut: 51](#_Toc182601304)

[3. Penilaian Sikap 51](#_Toc182601305)

[Skor 16-20 (Sangat Baik): Tindak Lanjut: 51](#_Toc182601306)

[Skor 11-15 (Baik): Tindak Lanjut: 51](#_Toc182601307)

[Skor 6-10 (Cukup): Tindak Lanjut: 52](#_Toc182601308)

[kerja sama dan tanggung jawab. 52](#_Toc182601309)

[Skor 1-5 (Kurang): Tindak Lanjut: 52](#_Toc182601310)

[Daftar Pustaka 52](#_Toc182601311)

[Glosarium 52](#_Toc182601312)

[1. Firewall: 52](#_Toc182601313)

[2. Proxy Server: 52](#_Toc182601314)

[3. VPN (Virtual Private Network): 53](#_Toc182601315)

[4. DDoS (Distributed Denial of Service): 53](#_Toc182601316)

[5. Port Scanning: 53](#_Toc182601317)

[6. IDS (Intrusion Detection System): 53](#_Toc182601318)

[7. IPS (Intrusion Prevention System): 53](#_Toc182601319)

[8. Stateful Firewall: 53](#_Toc182601320)

[9. Stateless Firewall: 53](#_Toc182601321)

[10. Least Privilege Principle: 53](#_Toc182601322)

[11. ACL (Access Control List): 53](#_Toc182601323)

[12. Encryption: 53](#_Toc182601324)

[13. Packet Filtering: 53](#_Toc182601325)

[14. VPN Tunnel: 53](#_Toc182601326)

# 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, Teknik Deteksi Ancaman, Manajemen Proxy Internal dan Eksternal |
| Kelas / Semester | XI / Genap |
| Tahun Pelajaran | 2023/2024 |
| Alokasi Waktu | 54 JP x 45 Menit |
| Jumlah Pertemuan | 18 TM x 3 JP |
| Kompetensi Awal | Peserta didik diharapkan sudah memahami konsep dasar jaringan komputer dan pengenalan beberapa perangkat jaringan. |

# Profil Pelajar Pancasila

* 1. 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.

* 1. 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)
     1. Fasilitas Kelas

**Ruang Kelas** yang dilengkapi dengan sistem pencahayaan yang baik, ventilasi yang memadai, dan kursi meja yang nyaman untuk diskusi dan praktik.

**Proyektor dan Layar Proyeksi** untuk mempresentasikan 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.

* + 1. 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** sebagai perangkat lunak simulasi untuk konfigurasi firewall dan proxy.

**Ubuntu Server** atau sistem operasi lain yang mendukung pengelolaan proxy server (misalnya, Squid Proxy) dan VPN.

### Perangkat Jaringan:

Router dan switch untuk mendemonstrasikan pengaturan jaringan dan konektivitas. Kabel jaringan (LAN) untuk menghubungkan perangkat dalam jaringan lokal.

* + 1. 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 (Local Area Network)** untuk menghubungkan perangkat di dalam kelas dan memastikan akses ke jaringan lokal untuk simulasi dan praktik pengelolaan firewall dan proxy.

* + 1. 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, khususnya untuk mengamati potensi ancaman dan lalu lintas yang mencurigakan.

* 1. Prasarana (Fasilitas Pendukung)
     1. Ruang Praktikum

**Lab Komputer** yang dilengkapi dengan komputer yang telah terpasang Mikrotik RouterOS, Ubuntu Server, serta perangkat lunak untuk konfigurasi dan pengelolaan jaringan lainnya.

**Koneksi Jaringan** untuk menghubungkan semua perangkat di dalam ruang praktikum untuk membangun simulasi jaringan yang aman.

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

* + 1. Jaringan dan Infrastruktur

**Jaringan Wi-Fi dan LAN** untuk menghubungkan seluruh perangkat di kelas atau ruang praktikum sehingga peserta didik bisa melakukan percakapan antar perangkat jaringan dan mengakses materi atau referensi.

**Perangkat Jaringan Mikrotik** yang dapat digunakan 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 mengimplementasikan kebijakan kontrol akses dan pengelolaan lalu lintas.

* + 1. Perangkat Monitoring dan Pengawasan\*\*

**Software Monitoring Jaringan** (misalnya, **Wireshark** atau **PRTG Network Monitor**) 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.

* + 1. 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, berupa materi yang diunduh dari berbagai sumber terpercaya terkait topik-topik seperti pengaturan firewall pada Mikrotik, konfigurasi proxy server pada Ubuntu, serta mitigasi ancaman DDoS dan port scanning.

* + 1. Ketersediaan Fasilitas Tambahan\*\*

**Laboratorium Keamanan Jaringan (Opsional)**: Sebuah ruang yang dikhususkan untuk melakukan ujian praktek dengan perangkat keras dan perangkat lunak jaringan yang lebih canggih dan lebih besar skalanya. Ideal untuk praktik secara nyata dengan kondisi yang mendekati jaringan yang ada di dunia industri.

### Fasilitas Penunjang Lainnya:

**Kamera untuk Demo Praktek**: Agar peserta didik bisa mengikuti setiap tahapan dengan jelas dan dapat diulang untuk mempelajari lebih dalam.

**Whiteboard Digital atau Smartboard** untuk memberikan penjelasan yang lebih interaktif dan menampilkan konfigurasi secara langsung.

# Target Peserta Didik

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

1. Peserta Didik Reguler/Tipikal:

**Karakteristik**: Peserta didik pada kategori ini memiliki kemampuan untuk memahami dan mencerna materi ajar dengan mudah. Mereka dapat mengikuti pelajaran dengan baik dan tidak mengalami kesulitan dalam memahami konsep-konsep dasar maupun teknik-teknik praktis yang diajarkan, seperti konfigurasi firewall, proxy, dan VPN.

**Pendekatan Pembelajaran**: Pembelajaran diberikan dengan cara yang sistematis dan logis, menggunakan berbagai sumber daya (seperti video, PowerPoint, dan buku) untuk mendalami konsep-konsep dasar dan aplikasinya. Peserta didik ini dapat dengan cepat menguasai materi yang disampaikan dalam waktu yang relatif singkat.

1. Peserta Didik dengan Kesulitan Belajar:

**Karakteristik**: Peserta didik ini cenderung memiliki keterbatasan dalam gaya belajar (misalnya hanya dapat belajar dengan menggunakan media audio atau video). Mereka mungkin mengalami kesulitan dalam memahami materi ajar, sering merasa kurang percaya diri, serta menghadapi tantangan dalam konsentrasi jangka panjang.

Keterampilan pemecahan masalah dan pengelolaan waktu juga sering menjadi tantangan.

**Pendekatan Pembelajaran**: Untuk kategori ini, pendekatan pembelajaran yang lebih individual diperlukan. Penggunaan media seperti **video tutorial** dan **audio** sangat disarankan untuk membantu mereka memahami materi dengan lebih mudah. Peserta didik ini juga mungkin membutuhkan waktu lebih lama dan dukungan tambahan, seperti bimbingan pribadi dan kesempatan untuk mengulang materi atau latihan dengan cara yang lebih interaktif.

* + 1. Peserta Didik dengan Pencapaian Tinggi:

**Karakteristik**: Peserta didik ini cepat mencerna dan memahami materi ajar serta mampu menerapkannya dengan sangat baik. Mereka mampu mencapai keterampilan berpikir tingkat tinggi (HOTS) dan dapat memimpin diskusi serta menyelesaikan masalah yang lebih kompleks. Mereka tidak hanya memahami konsep, tetapi juga mampu mengembangkan solusi praktis serta mengaplikasikan keterampilan yang dipelajari dalam konteks dunia nyata.

**Pendekatan Pembelajaran**: Untuk peserta didik dengan pencapaian tinggi, pendekatan yang lebih menantang dan berbasis **proyek** atau **tugas-tugas yang memerlukan kreativitas** dan **pemecahan masalah kompleks** sangat dianjurkan. Mereka dapat diberikan **studi kasus** atau tantangan yang memotivasi mereka untuk menggunakan kemampuan analitis dan inovatif mereka. Kesempatan untuk **berkolaborasi dalam proyek kelompok** juga akan membantu mereka mengembangkan keterampilan kepemimpinan dan kemampuan untuk mengelola tim.

## Pendekatan Pembelajaran yang Terintegrasi:

Untuk memastikan bahwa semua peserta didik dapat berkembang sesuai dengan kemampuannya, metode pembelajaran akan mengintegrasikan pendekatan berbasis **diferensiasi**. Hal ini memungkinkan setiap peserta didik mendapatkan pengalaman belajar yang sesuai dengan gaya belajar mereka, serta memberikan tantangan dan dukungan yang dibutuhkan.

**Peserta didik reguler/typical** akan diajak untuk mengikuti pembelajaran yang lebih cepat dan mendalam, dengan fokus pada penguasaan keterampilan teknis.

**Peserta didik dengan kesulitan belajar** akan didukung dengan media yang beragam dan pendekatan yang lebih personal, serta diberi kesempatan untuk mengulang materi dalam tempo yang lebih lambat.

**Peserta didik dengan pencapaian tinggi** akan diberikan tantangan yang lebih kompleks, serta kesempatan untuk memimpin diskusi dan proyek kelompok.

# Model Pembelajaran: Keamanan Jaringan

Model pembelajaran yang digunakan untuk materi **Keamanan Jaringan**, termasuk pengelolaan **Firewall**, **Proxy**, **VPN**, serta **Deteksi dan Mitigasi Ancaman**, harus mencakup pendekatan yang dapat mendukung keberagaman gaya belajar peserta didik. Berikut adalah **Model Pembelajaran yang Terintegrasi** untuk memastikan pemahaman dan keterampilan praktis dalam topik ini.

## Model Pembelajaran: Blended Learning (Pembelajaran Campuran)

**Blended Learning** adalah model yang menggabungkan pembelajaran tatap muka (face-to-face) dengan pembelajaran online, yang memungkinkan peserta didik untuk belajar secara mandiri dan berkolaborasi secara aktif dengan rekan-rekannya, sambil mendapatkan bimbingan langsung dari pendidik.

### Sesi Tatap Muka (Offline):

Fokus pada **praktik langsung**, seperti pengaturan firewall di Mikrotik, konfigurasi proxy server, serta pengelolaan VPN.

**Diskusi dan kolaborasi**: Peserta didik berdiskusi tentang tantangan yang mereka hadapi saat mengonfigurasi perangkat dan kebijakan keamanan.

**Studi Kasus**: Diskusi kelompok mengenai studi kasus serangan jaringan dan penerapan mitigasi ancaman.

### Sesi Online (Online Learning):

**Video Tutorial**: Peserta didik menonton video yang menjelaskan cara mengonfigurasi firewall dan proxy, serta teknik mitigasi ancaman.

**Google Classroom**: Materi ajar, tugas, dan ujian diunggah di platform ini. Peserta didik dapat mengakses materi kapan saja.

**Simulasi Online**: Peserta didik dapat melakukan **simulasi pengelolaan jaringan** menggunakan perangkat virtual untuk praktik deteksi ancaman dan mitigasi serangan.

### Keuntungan Blended Learning:

Mengakomodasi peserta didik dengan gaya belajar yang berbeda (visual, audio, kinestetik).

Memberikan fleksibilitas dalam belajar, memungkinkan peserta didik untuk belajar dengan kecepatan mereka sendiri. Mempermudah pendidik untuk memberikan umpan balik langsung dan dukungan personal.

## Model Pembelajaran: Problem-Based Learning (PBL)

**Problem-Based Learning (PBL)** adalah pendekatan yang berfokus pada pemecahan masalah dunia nyata, yang dapat melibatkan pengelolaan keamanan jaringan dalam konteks situasi yang lebih kompleks dan aplikatif.

### Fase 1: Identifikasi Masalah

Peserta didik diberikan **studi kasus nyata** atau simulasi masalah keamanan jaringan (misalnya, serangan DDoS atau kebocoran data melalui proxy).

Mereka diminta untuk **menganalisis masalah** dan **mengidentifikasi ancaman** yang terjadi dalam jaringan.

### Fase 2: Penyelesaian Masalah

Peserta didik bekerja dalam kelompok untuk **mencari solusi**, misalnya dengan mengonfigurasi firewall untuk mengatasi DDoS, atau mengatur proxy untuk membatasi akses ke situs berbahaya.

Pendidik membimbing kelompok untuk mencari informasi dan sumber daya yang relevan, baik secara online (misalnya melalui video tutorial atau artikel) maupun melalui diskusi kelompok.

### Fase 3: Presentasi Solusi

Setiap kelompok **mempresentasikan solusi** yang mereka temukan dan bagaimana solusi tersebut diterapkan dalam konteks dunia nyata.

Peserta didik menjelaskan cara mengonfigurasi firewall, proxy, dan VPN untuk mengatasi masalah yang diberikan.

### Keuntungan PBL:

Meningkatkan keterampilan **berpikir kritis** dan **problem-solving**. Mendorong **kolaborasi** antara peserta didik.

Membantu peserta didik melihat aplikasi praktis dari teori yang dipelajari dalam konteks dunia nyata.

## Model Pembelajaran: Project-Based Learning (PjBL)

**Project-Based Learning (PjBL)** adalah model pembelajaran yang berfokus pada pembuatan proyek nyata yang menggabungkan keterampilan teknis dan non-teknis, serta penerapan pengetahuan yang dipelajari dalam pembelajaran.

### Fase 1: Perencanaan Proyek

Peserta didik diberi **proyek pengelolaan jaringan** yang mencakup pengaturan firewall, proxy, dan VPN untuk sebuah perusahaan atau organisasi.

Mereka harus merencanakan **struktur jaringan** yang aman, termasuk penentuan kebijakan akses dan mitigasi ancaman.

### Fase 2: Pelaksanaan Proyek

Peserta didik bekerja dalam kelompok untuk **mengonfigurasi jaringan**, melakukan pengujian terhadap keamanan jaringan, dan **mengidentifikasi kerentanannya**.

Mereka dapat melakukan simulasi serangan dan menguji kebijakan keamanan yang telah diterapkan.

### Fase 3: Evaluasi dan Presentasi Proyek

Peserta didik diminta untuk **menyusun laporan proyek** yang mencakup analisis, konfigurasi yang dilakukan, serta solusi yang diterapkan untuk mengatasi masalah keamanan.

Presentasi proyek dilakukan di depan kelas atau dihadapan guru dan teman-teman mereka, untuk memaparkan temuan dan solusi yang diterapkan.

### Keuntungan PjBL:

Meningkatkan **keterampilan kerja tim** dan **kolaborasi**.

Membantu peserta didik mengembangkan keterampilan teknis dan **kreativitas** dalam menyelesaikan masalah. Meningkatkan **kemampuan presentasi** dan **komunikasi** dalam menyampaikan hasil kerja mereka.

## Model Pembelajaran: Direct Instruction (Instruksi Langsung)

**Direct Instruction** adalah model pembelajaran yang berfokus pada pengajaran langsung oleh guru, dengan penjelasan yang jelas dan rinci, serta diikuti dengan **latihan terstruktur**.

### Fase 1: Penjelasan Teori

Pendidik memberikan penjelasan tentang **konsep-konsep dasar keamanan jaringan**, seperti firewall, proxy, VPN, serta ancaman yang dapat terjadi pada jaringan. Penjelasan ini dilakukan dengan bantuan **slide PowerPoint** dan **video tutorial**.

### Fase 2: Demonstrasi Praktik

Pendidik mendemonstrasikan cara **mengonfigurasi firewall** menggunakan Mikrotik atau Ubuntu, serta cara mengonfigurasi proxy dan VPN di jaringan.

### Fase 3: Latihan Mandiri

Peserta didik diminta untuk **mengikuti langkah-langkah** yang telah dijelaskan dalam praktik dan mencoba mengonfigurasi jaringan mereka sendiri di perangkat Mikrotik dan Ubuntu.

### Keuntungan Direct Instruction:

Memberikan **pengetahuan dasar** yang kuat dan terstruktur.

Mudah untuk **memantau kemajuan** setiap peserta didik, terutama dalam praktik teknis.

Mengurangi kemungkinan peserta didik merasa bingung atau tertinggal dalam memahami konsep-konsep dasar.

Menggunakan kombinasi model **Blended Learning**, **Problem-Based Learning**, **Project-Based Learning**, dan **Direct Instruction** memungkinkan pendidik untuk:

**Menyesuaikan pendekatan** dengan kebutuhan beragam peserta didik. Meningkatkan keterampilan praktis dalam **keamanan jaringan**.

Mendorong **kolaborasi**, **pemecahan masalah**, serta **pemahaman yang mendalam** terhadap penerapan teknik-teknik yang telah dipelajari.

Dengan pendekatan-pendekatan ini, peserta didik tidak hanya mempelajari teori, tetapi juga memiliki kesempatan untuk

**menerapkan keterampilan** mereka dalam dunia nyata dan memperoleh **pengalaman langsung** dalam mengelola jaringan yang aman.

# Pemahaman Bermakna

## Pemahaman Bermakna dalam Pembelajaran Keamanan Jaringan

**Pemahaman Bermakna** mengacu pada pemahaman yang mendalam dan aplikatif, yang memungkinkan peserta didik untuk tidak hanya menghafal konsep-konsep tetapi juga mampu **menerapkan pengetahuan tersebut dalam situasi nyata**. Dalam konteks pembelajaran **Keamanan Jaringan**, pemahaman bermakna terjadi ketika peserta didik dapat menghubungkan konsep-konsep yang dipelajari dengan tantangan dunia nyata yang dihadapi dalam mengelola dan mengamankan jaringan. Mereka tidak hanya belajar **cara mengonfigurasi firewall** atau **proxy**, tetapi juga mengerti **mengapa** pengaturan tersebut diperlukan untuk melindungi data dan mencegah ancaman yang mungkin terjadi.

### Keterkaitan dengan Dunia Nyata:

Peserta didik dapat mengaitkan materi tentang **firewall**, **proxy**, **VPN**, dan **deteksi ancaman** dengan situasi dunia nyata, seperti perlindungan terhadap **data pribadi**, **keamanan transaksi online**, dan **perang dunia maya**. Misalnya, setelah belajar tentang firewall, peserta didik dapat memahami mengapa sebuah perusahaan atau institusi harus mengonfigurasi firewall mereka dengan cermat untuk **menghalau akses tidak sah** atau **serangan DDoS**.

### Penerapan Pengetahuan pada Masalah Praktis:

Pemahaman bermakna muncul ketika peserta didik mampu **menerapkan teori** yang mereka pelajari untuk

**menyelesaikan masalah praktis**. Misalnya, saat melakukan konfigurasi firewall atau proxy pada Mikrotik atau Ubuntu, peserta didik tidak hanya mengikuti langkah-langkah instruksi, tetapi mereka memahami **mengapa** setiap aturan firewall atau pengaturan proxy yang dilakukan itu penting dan **apa akibatnya jika salah konfigurasi**.

### Pengembangan Keterampilan Berpikir Kritis dan Analitis:

Pemahaman bermakna juga ditunjukkan dengan kemampuan peserta didik untuk berpikir secara **kritikal** dalam mengidentifikasi ancaman jaringan yang lebih kompleks dan **menyusun solusi mitigasi** yang sesuai. Mereka dapat menganalisis lalu lintas data dalam **monitoring jaringan** dan **menggunakan hasil analisis untuk menyesuaikan kebijakan keamanan**.

### Kemampuan Beradaptasi dengan Situasi yang Berubah:

Dalam dunia **keamanan jaringan**, ancaman dan teknologi berkembang pesat. Peserta didik dengan pemahaman bermakna dapat **beradaptasi dengan cepat** terhadap perubahan dan memahami **teknologi baru** atau **ancaman baru**. Misalnya, mereka dapat mengonfigurasi perangkat Mikrotik untuk menangani **serangan terbaru** atau mengoptimalkan penggunaan **VPN** di perusahaan yang menerapkan **kerja jarak jauh**.

### Keterlibatan Aktif dalam Proses Pembelajaran:

Pemahaman bermakna tercipta ketika peserta didik aktif terlibat dalam diskusi, percakapan, dan kegiatan praktik. Misalnya, melalui **simulasi serangan** dan **deteksi ancaman** yang dilakukan di ruang kelas atau melalui **studi kasus dunia nyata**, mereka tidak hanya memahami teorinya tetapi juga dapat **mengimplementasikannya secara langsung**.

## Contoh Pemahaman Bermakna pada Materi Keamanan Jaringan**:**

### Firewall:

**Konsep**: Peserta didik memahami bahwa firewall bertindak sebagai **penjaga gerbang** yang menyaring dan mengontrol akses ke dalam jaringan.

**Pemahaman Bermakna**: Peserta didik memahami **perbedaan antara stateful dan stateless firewall** dan dapat mengidentifikasi jenis firewall mana yang lebih cocok untuk kebutuhan jaringan tertentu. Mereka juga bisa mengonfigurasi firewall untuk **mengizinkan akses terbatas** atau **memblokir akses berbahaya** pada jaringan yang mereka kelola.

### Proxy Server:

**Konsep**: Proxy server berfungsi untuk **mengelola lalu lintas internet** dengan bertindak sebagai perantara antara pengguna dan internet.

**Pemahaman Bermakna**: Peserta didik mengerti bahwa **proxy server** dapat digunakan untuk **menyaring konten**, **mengontrol akses** ke internet, dan **melindungi privasi** pengguna. Mereka dapat mengonfigurasi proxy untuk

### mencegah akses ke situs berbahaya atau mengatur penggunaan internet di organisasi.

1. VPN (Virtual Private Network):

**Konsep**: VPN menyediakan **akses aman ke jaringan lokal** melalui jaringan publik seperti internet, mengenkripsi data yang dikirimkan agar aman.

**Pemahaman Bermakna**: Peserta didik tidak hanya tahu cara mengonfigurasi VPN, tetapi juga **memahami pentingnya keamanan enkripsi** dalam melindungi data sensitif saat melakukan transaksi atau akses jaringan dari lokasi yang jauh. Mereka dapat menilai kapan dan mengapa sebuah organisasi perlu menerapkan **VPN** untuk mendukung **kerja jarak jauh**.

### Deteksi dan Mitigasi Ancaman:

**Konsep**: Peserta didik belajar tentang cara **mendeteksi ancaman** pada jaringan menggunakan tools seperti

**Wireshark** atau **Mikrotik Torch** dan cara melakukan **mitigasi** terhadap ancaman yang terdeteksi.

**Pemahaman Bermakna**: Peserta didik dapat **menganalisis lalu lintas data**, mengenali tanda-tanda serangan seperti **DDoS**, dan mengetahui langkah mitigasi yang harus diambil untuk **memblokir serangan** tersebut atau **memperbaiki kerentanannya**.

Keamanan jaringan bukan hanya tentang mengonfigurasi perangkat dan mengikuti prosedur. Itu juga tentang **pemahaman konteks dan aplikasi dunia nyata**. Peserta didik yang memiliki pemahaman bermakna akan:

**Dapat beradaptasi** dengan ancaman baru yang muncul.

**Mengidentifikasi dan menyelesaikan masalah** yang lebih kompleks dengan cara yang kreatif.

**Memiliki rasa tanggung jawab** terhadap keamanan data dan jaringan mereka, serta dapat mengimplementasikan solusi yang sesuai untuk melindungi informasi sensitif.

Dengan pendekatan pembelajaran yang mendorong pemahaman bermakna, peserta didik tidak hanya memperoleh keterampilan teknis, tetapi juga membangun kemampuan berpikir kritis dan **mempersiapkan diri untuk tantangan dunia nyata** dalam mengelola keamanan jaringan.

# Pertanyaan Pemantik

### Tentang Firewall:

Mengapa firewall penting dalam melindungi jaringan komputer?

Apa perbedaan antara **firewall stateful** dan **stateless**? Kapan masing-masing lebih efektif digunakan?

Jika Anda memiliki sebuah jaringan di perusahaan kecil, jenis firewall apa yang akan Anda pilih dan mengapa?

### Tentang Proxy Server:

Apa yang dimaksud dengan **proxy server**, dan bagaimana cara kerjanya dalam sebuah jaringan? Mengapa banyak perusahaan menggunakan **proxy server** untuk mengelola akses internet penggunanya? Bagaimana **proxy server** dapat membantu dalam meningkatkan **keamanan** dan **kinerja jaringan**?

### Tentang VPN:

Apa itu **VPN (Virtual Private Network)** dan bagaimana cara kerjanya dalam mengamankan koneksi internet? Mengapa VPN penting bagi pekerja jarak jauh atau pengguna yang sering terhubung ke jaringan publik seperti Wi- Fi di kafe atau hotel?

Bagaimana VPN dapat **melindungi privasi** dan **mengamankan data pribadi** Anda saat mengakses internet?

### Tentang Deteksi dan Mitigasi Ancaman:

Apa itu **serangan DDoS** dan bagaimana dampaknya terhadap jaringan komputer?

Bagaimana Anda mendeteksi adanya **aktivitas mencurigakan** di jaringan menggunakan tools seperti **Wireshark**

atau **Mikrotik Torch**?

Jika jaringan Anda diserang, apa langkah pertama yang harus diambil untuk **mitigasi ancaman**?

### Tentang Kebijakan Keamanan Jaringan:

Mengapa **kebijakan akses** penting dalam sebuah jaringan? Apa saja yang perlu dipertimbangkan dalam menyusun kebijakan akses yang baik?

Bagaimana Anda mengelola hak akses pengguna di sebuah **jaringan besar** agar tetap aman dan efisien?

Dalam konteks kebijakan keamanan, apa yang dimaksud dengan **least privilege principle** dan bagaimana prinsip ini diterapkan dalam pengelolaan firewall atau VPN?

## Tujuan Penggunaan Pertanyaan Pemantik**:**

**Menggugah rasa ingin tahu** peserta didik tentang konsep-konsep dasar dalam keamanan jaringan.

**Mendorong diskusi** mengenai **peran penting** firewall, proxy, VPN, dan mitigasi ancaman dalam menjaga keamanan jaringan.

**Meningkatkan kesadaran** peserta didik mengenai **ancaman dunia nyata** yang dapat mengganggu keamanan data dan sistem mereka.

# Kompetensi Inti

|  |  |
| --- | --- |
| **Komponen** | **Detail** |
| **Capaian**  **Pembelajaran** | Pada akhir fase F, peserta didik mampu memahami dan menerapkan konsep keamanan jaringan, mengidentifikasi jenis ancaman dan kerentanan dalam jaringan, serta menerapkan teknik deteksi dan mitigasi untuk mencegah dan mengatasi insiden keamanan jaringan. Peserta didik juga diharapkan mampu menyusun laporan dan mempresentasikan hasil analisis studi kasus keamanan jaringan. |
| **Tujuan**  **Pembelajaran** | 1. Memahami konsep dasar keamanan jaringan. 2. Mengenali dan mengidentifikasi ancaman dan kerentanan dalam jaringan. 3. Menerapkan teknik deteksi ancaman jaringan. 4. Menggunakan teknik mitigasi untuk mengamankan jaringan. 5. Menerapkan konfigurasi proxy internal dan eksternal menggunakan Mikrotik dan Ubuntu. 6. Menganalisis dan menyusun laporan insiden keamanan. 7. Mempresentasikan hasil analisis keamanan jaringan. |
| **Bukti**  **Ketercapaian** | 1. Praktik konfigurasi firewall dan proxy. 2. Laporan hasil analisis keamanan jaringan. 3. Presentasi hasil analisis dan solusi mitigasi ancaman. 4. Ujian praktek konfigurasi jaringan dan deteksi ancaman. |
| **Asesmen** | 1. Ujian teori mengenai konsep dasar keamanan jaringan dan jenis ancaman. 2. Penilaian tugas individu berupa laporan analisis insiden keamanan jaringan. 3. Ujian praktek mengenai konfigurasi firewall, proxy, dan teknik mitigasi ancaman. 4. Penilaian presentasi hasil analisis keamanan jaringan. |
| **Pemahaman Bermakna** | Peserta didik dapat menghubungkan konsep dasar keamanan jaringan dengan praktik nyata dalam melindungi jaringan dari ancaman, serta mampu menyusun kebijakan dan langkah mitigasi yang sesuai dengan kebutuhan jaringan yang dipelajari. Peserta didik diharapkan dapat mengimplementasikan pengetahuan yang didapat dalam simulasi jaringan yang aman dan terlindungi dengan menggunakan berbagai alat dan teknik yang sesuai. |

## 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. Pendidik memberikan kesempatan kepada beberapa peserta didik untuk menceritakan perasaannya dan peserta didik lain diminta untuk memberikan tanggapan yang positif. 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. Apakah kalian sudah tahu apa itu firewall?    2. Apakah kalian sudah tahu fungsi dari firewall dalam jaringan? |
| **Kegiatan Inti (135 Menit)** | 1. Peserta didik dikelompokkan menjadi beberapa kelompok heterogen untuk melakukan diskusi mengenai firewall dan perannya dalam keamanan jaringan. 2. Peserta didik diberikan stimulus dalam bentuk tayangan video tentang pengantar firewall dan fungsinya dalam jaringan. [Video Pengantar Firewall](https://youtu.be/QlT5fEPhmBI) 3. Pendidik menjelaskan materi dengan memberikan beberapa link video terkait firewall:    * [Definisi dan Fungsi Firewall](https://youtu.be/pKJmb04T0FQ)    * [Jenis-Jenis Firewall](https://youtu.be/LE8AHJacCFM)    * [Buku Elektronik: Konsep Dasar Firewall](https://www.academia.edu/16832625/Pemrograman_web_statis_dan_dinamis) 4. Peserta didik melakukan diskusi dan saling membantu memahami konsep dasar firewall. 5. Setiap kelompok diminta untuk menyimpulkan dan merangkum konsep dasar firewall serta manfaatnya. 6. Peserta didik menggali dan menemukan contoh penerapan firewall di kehidupan nyata. 7. Peserta didik mendiskusikan implementasi firewall di jaringan sekolah atau rumah. 8. Masing-masing kelompok mempresentasikan hasil diskusinya menggunakan media pilihan seperti PowerPoint, gambar, atau naskah cerita. |

|  |  |
| --- | --- |
| **Kegiatan**  **Pembelajaran** | **Deskripsi** |
|  | 1. Pendidik meminta kelompok lain memberikan tanggapan terhadap presentasi kelompok   lainnya.   1. Setiap kelompok mencatat masukan dan memperbaiki presentasi mereka. 2. Pendidik meminta setiap kelompok mengumpulkan hasil presentasi yang sudah disempurnakan. |
| **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 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? | [ ] | [ ] | [ ] |
| 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.
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 "Pengertian dan Fungsi Firewall": [Pengertian Firewall](https://youtu.be/pKJmb04T0FQ). Video tema "Jenis-Jenis Firewall": [Jenis-jenis Firewall](https://youtu.be/LE8AHJacCFM).

Buku Elektronik Penunjang Belajar: [Pemrograman Web untuk Pemula](https://www.academia.edu/16832625/Pemrograman_web_statis_dan_dinamis).

Glosarium

1. Firewall: Sistem keamanan jaringan yang berfungsi untuk memantau dan mengontrol lalu lintas jaringan berdasarkan aturan yang telah ditentukan.
2. Packet Filtering: Proses memfilter data yang lewat berdasarkan aturan yang telah ditetapkan, yang digunakan dalam firewall.
3. Stateful Inspection: Teknik firewall yang melacak status koneksi aktif dan memeriksa apakah paket data sesuai dengan status tersebut.
4. Proxy: Server perantara yang digunakan untuk mengontrol akses ke sumber daya di luar jaringan internal.

Daftar Pustaka

1. Dicoding, "Ngoding Web Dinamis Atau Statis", 15 Januari 2020, [dicoding.com](https://www.dicoding.com/blog/ngoding-web-dinamis-atau-statis/).
2. Dewaweb, "Perbedaan Web Statis dan Web Dinamis", 27 Mei 2022, [dewaweb.com](https://dewaweb.com/).
3. Santoso, A. (2019). Pemrograman Web untuk Pemula. Informatika 7 in 1 Pemrograman Web untuk Pemula - Rohi Abdulloh - Google Buku.

## 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 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 kalian ketahui tentang arsitektur firewall?    2. Apa perbedaan antara firewall berbasis perangkat keras dan perangkat lunak? |
| **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 tentang konsep dasar arsitektur dan desain firewall. [Video Arsitektur dan Desain Firewall](https://youtu.be/QlT5fEPhmBI) 3. Pendidik menjelaskan materi mengenai arsitektur dan desain firewall, serta jenis-jenis firewall yang sering digunakan dalam pengamanan jaringan. 4. Pendidik memberikan referensi video tentang firewall berbasis perangkat keras dan perangkat lunak:    * [Firewall Berbasis Perangkat Keras](https://youtu.be/pKJmb04T0FQ)    * [Firewall Berbasis Perangkat Lunak](https://youtu.be/LE8AHJacCFM) 5. Peserta didik melakukan diskusi dalam kelompok untuk membahas berbagai arsitektur firewall yang digunakan dalam organisasi atau perusahaan. 6. Peserta didik diminta untuk menyimpulkan dan merangkum jenis-jenis firewall dan arsitektur yang sesuai dengan kebutuhan jaringan yang berbeda. 7. Peserta didik menggali dan menemukan contoh penerapan arsitektur firewall dalam kehidupan sehari-hari, seperti di rumah atau di kantor. 8. Peserta didik mendiskusikan penerapan desain firewall dalam skala kecil dan besar, serta tantangan yang mungkin dihadapi. 9. Masing-masing kelompok mempresentasikan hasil diskusinya menggunakan media yang telah disiapkan seperti PowerPoint, video, atau naskah cerita. 10. Pendidik meminta kelompok lain untuk memberikan tanggapan terhadap presentasi kelompok lainnya. 11. Setiap kelompok mencatat masukan dan memperbaiki presentasi mereka. 12. Pendidik meminta kelompok mengumpulkan hasil presentasi yang sudah disempurnakan sesuai media yang mereka pilih. |
| **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 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.
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 "Pengertian dan Fungsi Firewall": [Pengertian Firewall](https://youtu.be/pKJmb04T0FQ). Video tema "Arsitektur dan Desain Firewall": [Arsitektur Firewall](https://youtu.be/LE8AHJacCFM).

Buku Elektronik Penunjang Belajar: [Desain Firewall](https://www.academia.edu/16832625/Pemrograman_web_statis_dan_dinamis).

Glosarium

1. Firewall Berbasis Perangkat Keras: Firewall yang berupa perangkat fisik yang berfungsi untuk memfilter dan mengontrol lalu lintas jaringan.
2. Firewall Berbasis Perangkat Lunak: Firewall yang berupa aplikasi yang dijalankan pada sistem operasi untuk mengontrol lalu lintas data.
3. Stateful Inspection: Teknik firewall yang memeriksa status setiap paket data dan membandingkannya dengan status koneksi yang aktif.
4. Proxy: Server perantara yang digunakan untuk menyaring lalu lintas data yang masuk dan keluar dari jaringan internal.

Daftar Pustaka

1. Dicoding, "Ngoding Web Dinamis Atau Statis", 15 Januari 2020, [dicoding.com](https://www.dicoding.com/blog/ngoding-web-dinamis-atau-statis/).
2. Dewaweb, "Perbedaan Web Statis dan Web Dinamis", 27 Mei 2022, [dewaweb.com](https://dewaweb.com/).
3. Santoso, A. (2019). Pemrograman Web untuk Pemula. Informatika 7 in 1 Pemrograman Web untuk Pemula - Rohi Abdulloh - Google Buku.

## 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. Pendidik memberikan kesempatan kepada beberapa peserta didik untuk membahas materi pertemuan sebelumnya tentang arsitektur dan desain firewall. 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 packet filtering?    2. Mengapa packet filtering penting dalam 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 konsep packet filtering dan penerapannya pada perangkat Mikrotik. [Video Packet Filtering](https://youtu.be/QlT5fEPhmBI) 3. Pendidik menjelaskan materi tentang packet filtering menggunakan Mikrotik dan bagaimana konfigurasi dasar dilakukan untuk mengontrol lalu lintas data. 4. Pendidik memberikan referensi video yang menjelaskan cara konfigurasi packet filtering di Mikrotik:    * [Packet Filtering di Mikrotik](https://youtu.be/LE8AHJacCFM)    * Buku Elektronik Penunjang: [Konfigurasi Mikrotik](https://www.academia.edu/16832625/Pemrograman_web_statis_dan_dinamis) 5. Peserta didik melakukan latihan konfigurasi dasar packet filtering di Mikrotik. 6. Peserta didik mendiskusikan penerapan packet filtering untuk mengamankan jaringan lokal di rumah atau sekolah. 7. Peserta didik diminta untuk menyusun dan merangkum cara konfigurasi packet filtering dengan Mikrotik serta manfaatnya. 8. Masing-masing kelompok mempresentasikan hasil latihan dan diskusi mereka menggunakan media seperti PowerPoint atau video tutorial. 9. Pendidik meminta kelompok lain untuk memberikan tanggapan terhadap presentasi kelompok lainnya. 10. Setiap kelompok mencatat masukan dan memperbaiki presentasi mereka. 11. 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 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? | [ ] |

|  |  |  |
| --- | --- | --- |
| **No** | **Pertanyaan** | **Jawaban** |
| 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 "Pengertian dan Konfigurasi Packet Filtering di Mikrotik": [Packet Filtering Mikrotik](https://youtu.be/LE8AHJacCFM). Buku Elektronik Penunjang Belajar: [Konfigurasi Mikrotik](https://www.academia.edu/16832625/Pemrograman_web_statis_dan_dinamis).

Glosarium

1. Packet Filtering: Teknik untuk memfilter paket data yang masuk atau keluar jaringan berdasarkan aturan yang sudah ditentukan. Digunakan untuk meningkatkan keamanan jaringan.
2. Mikrotik: Perangkat jaringan yang digunakan untuk mengatur berbagai macam konfigurasi jaringan, termasuk firewall dan packet filtering.
3. Firewall: Sistem yang digunakan untuk mengontrol akses jaringan dan melindungi jaringan dari ancaman luar dengan memfilter lalu lintas data.
4. Stateful Inspection: Metode inspeksi yang memeriksa status koneksi sebelum memperbolehkan paket data masuk ke dalam jaringan.

Daftar Pustaka

1. Dicoding, "Ngoding Web Dinamis Atau Statis", 15 Januari 2020, [dicoding.com](https://www.dicoding.com/blog/ngoding-web-dinamis-atau-statis/).
2. Dewaweb, "Perbedaan Web Statis dan Web Dinamis", 27 Mei 2022, [dewaweb.com](https://dewaweb.com/).
3. Santoso, A. (2019). Pemrograman Web untuk Pemula. Informatika 7 in 1 Pemrograman Web untuk Pemula - Rohi Abdulloh - Google Buku.

## 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. Pendidik memberikan kesempatan kepada beberapa peserta didik untuk membahas materi pertemuan sebelumnya tentang packet filtering dan penerapannya menggunakan 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 aturan dasar yang perlu diterapkan dalam konfigurasi firewall?    2. Mengapa pengelolaan firewall 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 konsep dasar |

|  |  |
| --- | --- |
| **Kegiatan**  **Pembelajaran** | **Deskripsi** |
|  | pengelolaan firewall dan cara mengonfigurasi firewall pada Mikrotik. [Video Konfigurasi Firewall](https://youtu.be/LE8AHJacCFM)   1. Pendidik menjelaskan materi tentang konfigurasi dan pengelolaan firewall menggunakan Mikrotik, termasuk pengaturan kebijakan akses, pembuatan aturan firewall, dan pengelolaan log firewall. 2. Pendidik memberikan referensi video yang menjelaskan konfigurasi firewall pada Mikrotik:    * [Cara Konfigurasi Firewall Mikrotik](https://youtu.be/5gZkJtKz0N8)    * Buku Elektronik Penunjang: [Panduan Konfigurasi Mikrotik](https://www.academia.edu/16832625/Pemrograman_web_statis_dan_dinamis) 3. Peserta didik melakukan latihan konfigurasi firewall di Mikrotik dengan mengikuti langkah- langkah yang telah diajarkan. 4. Peserta didik melakukan analisis tentang pentingnya pengelolaan log firewall untuk pemantauan dan audit keamanan jaringan. 5. Peserta didik diminta untuk menyusun dan merangkum langkah-langkah konfigurasi dan pengelolaan firewall serta manfaatnya. 6. Masing-masing kelompok mempresentasikan hasil latihan dan diskusi mereka menggunakan media seperti PowerPoint, video tutorial, atau naskah cerita. 7. Pendidik meminta kelompok lain untuk memberikan tanggapan terhadap presentasi kelompok lainnya. 8. Setiap kelompok mencatat masukan dan memperbaiki presentasi mereka. 9. 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 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.
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 Firewall di Mikrotik": [Konfigurasi Mikrotik](https://youtu.be/5gZkJtKz0N8). Buku Elektronik Penunjang Belajar: [Panduan Mikrotik](https://www.academia.edu/16832625/Pemrograman_web_statis_dan_dinamis).

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.

Daftar Pustaka

1. Dicoding, "Ngoding Web Dinamis Atau Statis", 15 Januari 2020, [dicoding.com](https://www.dicoding.com/blog/ngoding-web-dinamis-atau-statis/).
2. Dewaweb, "Perbedaan Web Statis dan Web Dinamis", 27 Mei 2022, [dewaweb.com](https://dewaweb.com/).
3. Santoso, A. (2019). Pemrograman Web untuk Pemula. Informatika 7 in 1 Pemrograman Web untuk Pemula - Rohi Abdulloh - Google Buku.

## 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. Pendidik memberikan kesempatan kepada beberapa peserta didik untuk membahas materi pertemuan sebelumnya tentang konfigurasi dan pengelolaan firewall. 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. Mengapa monitoring dan logging penting dalam pengelolaan firewall?    2. Apa yang dimaksud dengan log firewall dan bagaimana cara membaca log tersebut? |
| **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 monitoring dan logging aktivitas firewall di Mikrotik. [Video Monitor dan Log Aktivitas Firewall](https://youtu.be/QlT5fEPhmBI) 3. Pendidik menjelaskan materi tentang cara memantau aktivitas firewall dan membaca log pada Mikrotik, termasuk cara menggunakan fitur monitoring dan log untuk mendeteksi ancaman. 4. Pendidik memberikan referensi video yang menjelaskan cara monitoring dan membaca log di Mikrotik:    * [Monitoring Aktivitas Firewall 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 mengaktifkan fitur logging dan monitoring pada Mikrotik serta menganalisis log yang dihasilkan. 6. Peserta didik diminta untuk menyusun dan merangkum langkah-langkah monitoring dan membaca log firewall serta manfaatnya. 7. Masing-masing kelompok mempresentasikan hasil latihan dan diskusi mereka menggunakan media seperti PowerPoint, video tutorial, atau naskah cerita. 8. Pendidik meminta kelompok lain untuk memberikan tanggapan terhadap presentasi kelompok lainnya. 9. Setiap kelompok mencatat masukan dan memperbaiki presentasi mereka. 10. Pendidik meminta kelompok untuk mengumpulkan hasil presentasi yang sudah disempurnakan sesuai media yang dipilih. |

|  |  |
| --- | --- |
| **Kegiatan**  **Pembelajaran** | **Deskripsi** |
| **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 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.
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 "Monitor dan Log Aktivitas Firewall Mikrotik": [Monitoring Firewall Mikrotik](https://youtu.be/LE8AHJacCFM). Buku Elektronik Penunjang Belajar: [Panduan Mikrotik dan Log Firewall](https://www.academia.edu/16832625/Pemrograman_web_statis_dan_dinamis).

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.

Daftar Pustaka

1. Dicoding, "Ngoding Web Dinamis Atau Statis", 15 Januari 2020, [dicoding.com](https://www.dicoding.com/blog/ngoding-web-dinamis-atau-statis/).
2. Dewaweb, "Perbedaan Web Statis dan Web Dinamis", 27 Mei 2022, [dewaweb.com](https://dewaweb.com/).
3. Santoso, A. (2019). Pemrograman Web untuk Pemula. Informatika 7 in 1 Pemrograman Web untuk Pemula - Rohi Abdulloh - Google Buku.

## 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. Pendidik memberikan kesempatan kepada beberapa peserta didik untuk membahas materi pertemuan sebelumnya tentang monitoring dan log aktivitas firewall. 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. Mengapa implementasi firewall dalam jaringan sangat penting?    2. Apa saja yang perlu diperhatikan saat mengimplementasikan firewall dalam jaringan besar dan kecil? |
| **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 implementasi firewall dalam jaringan menggunakan Mikrotik. [Video Implementasi Firewall Mikrotik](https://youtu.be/QlT5fEPhmBI) 3. Pendidik menjelaskan materi tentang penerapan firewall dalam berbagai jenis jaringan, baik jaringan kecil (rumah) maupun besar (perusahaan). 4. Pendidik memberikan referensi video yang menjelaskan penerapan firewall dalam skala jaringan besar:    * [Implementasi Firewall pada Jaringan Perusahaan](https://youtu.be/LE8AHJacCFM)    * Buku Elektronik Penunjang: [Panduan Mikrotik untuk Implementasi Firewall](https://www.academia.edu/16832625/Pemrograman_web_statis_dan_dinamis) 5. Peserta didik melakukan latihan penerapan firewall pada skenario jaringan rumah dan kantor kecil menggunakan Mikrotik. 6. Peserta didik melakukan diskusi mengenai tantangan yang dihadapi dalam mengimplementasikan firewall pada jaringan besar dan bagaimana cara mengatasinya. 7. Peserta didik diminta untuk menyusun dan merangkum langkah-langkah implementasi firewall serta tantangan yang mungkin dihadapi. 8. Masing-masing kelompok mempresentasikan hasil latihan dan diskusi mereka menggunakan media seperti PowerPoint, video tutorial, atau naskah cerita. 9. Pendidik meminta kelompok lain untuk memberikan tanggapan terhadap presentasi kelompok lainnya. 10. Setiap kelompok mencatat masukan dan memperbaiki presentasi mereka. 11. 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 mengimplementasikan firewall dalam jaringan? | [ ] | [ ] | [ ] |

|  |  |  |  |
| --- | --- | --- | --- |
| **Pertanyaan Refleksi** | **Baik** | **Cukup** | **Kurang** |
| 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? | [ ] |
| 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 "Implementasi Firewall pada Jaringan Mikrotik": [Implementasi Firewall Mikrotik](https://youtu.be/LE8AHJacCFM). Buku Elektronik Penunjang Belajar: [Panduan Mikrotik untuk Implementasi Firewall](https://www.academia.edu/16832625/Pemrograman_web_statis_dan_dinamis).

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.

Daftar Pustaka

1. Dicoding, "Ngoding Web Dinamis Atau Statis", 15 Januari 2020, [dicoding.com](https://www.dicoding.com/blog/ngoding-web-dinamis-atau-statis/).
2. Dewaweb, "Perbedaan Web Statis dan Web Dinamis", 27 Mei 2022, [dewaweb.com](https://dewaweb.com/).
3. Santoso, A. (2019). Pemrograman Web untuk Pemula. Informatika 7 in 1 Pemrograman Web untuk Pemula - Rohi Abdulloh - Google Buku.

## 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. Pendidik memberikan kesempatan kepada beberapa peserta didik untuk membahas materi pertemuan sebelumnya tentang implementasi firewall dalam 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 tantangan terbesar dalam mengelola firewall saat ini?    2. Apa saja tren terbaru dalam teknologi firewall yang perlu diperhatikan? |
| **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 tantangan dan tren terbaru dalam teknologi firewall. [Video Tantangan dan Tren Terbaru dalam Firewall](https://youtu.be/QlT5fEPhmBI) 3. Pendidik menjelaskan materi tentang tantangan yang dihadapi dalam mengelola firewall di era digital, serta tren terbaru dalam teknologi firewall seperti Next-Generation Firewall (NGFW) dan integrasi dengan sistem keamanan lainnya. 4. Pendidik memberikan referensi video tentang tren terbaru dalam firewall:    * [Next-Generation Firewall (NGFW) dan Keamanan Jaringan](https://youtu.be/LE8AHJacCFM)    * Buku Elektronik Penunjang: [Tren Terbaru dalam Keamanan Jaringan](https://www.academia.edu/16832625/Pemrograman_web_statis_dan_dinamis) 5. Peserta didik melakukan diskusi kelompok mengenai tantangan yang ada dalam firewall, seperti serangan DDoS, malware, dan masalah skalabilitas. 6. Peserta didik juga mendiskusikan tren terbaru dalam firewall, termasuk NGFW dan kemampuan integrasi dengan solusi keamanan lainnya, seperti sistem deteksi intrusi (IDS/IPS). 7. Peserta didik diminta untuk menyusun dan merangkum tantangan dan tren terbaru dalam teknologi firewall serta bagaimana solusi terbaru dapat membantu mengatasinya. 8. Masing-masing kelompok mempresentasikan hasil diskusi mereka menggunakan media seperti PowerPoint, video tutorial, atau naskah cerita. 9. Pendidik meminta kelompok lain untuk memberikan tanggapan terhadap presentasi kelompok lainnya. 10. Setiap kelompok mencatat masukan dan memperbaiki presentasi mereka. 11. 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 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.
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 "Next-Generation Firewall dan Keamanan Jaringan": [NGFW dalam Keamanan Jaringan](https://youtu.be/LE8AHJacCFM). Buku Elektronik Penunjang Belajar: [Tren Terbaru dalam Keamanan Jaringan](https://www.academia.edu/16832625/Pemrograman_web_statis_dan_dinamis).

Glosarium

1. Next-Generation Firewall (NGFW): Firewall generasi terbaru yang tidak hanya memfilter paket data, tetapi juga memiliki kemampuan untuk mendeteksi dan mencegah ancaman canggih, seperti malware dan serangan DDoS, serta dapat berintegrasi dengan solusi keamanan lainnya.
2. Serangan DDoS (Distributed Denial of Service): Serangan yang berusaha untuk membuat sebuah layanan tidak dapat diakses dengan membanjiri server atau jaringan dengan trafik yang sangat tinggi.
3. IDS/IPS (Intrusion Detection/Prevention System): Sistem yang digunakan untuk mendeteksi dan mencegah intrusi atau ancaman di jaringan dengan memonitor trafik dan mengambil tindakan untuk memblokir serangan.

Daftar Pustaka

1. Dewaweb, "Perbedaan Web Statis dan Web Dinamis", 27 Mei 2022, [dewaweb.com](https://dewaweb.com/).
2. Santoso, A. (2019). Pemrograman Web untuk Pemula. Informatika 7 in 1 Pemrograman Web untuk Pemula - Rohi Abdulloh - Google Buku.
3. Next-Generation Firewall (NGFW) Articles, "Tren Terbaru dalam Keamanan Jaringan", [cybersecurity-magazine.com](https://cybersecurity-magazine.com/).

## 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. Pendidik memberikan kesempatan kepada beberapa peserta didik untuk membahas materi pertemuan sebelumnya tentang firewall dan tantangan terkini dalam 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 proxy server?    2. Apa perbedaan antara proxy server dan firewall? |
| **Kegiatan Inti (135 Menit)** | 1. Peserta didik dikelompokkan menjadi beberapa kelompok yang telah dibentuk di pertemuan sebelumnya. |

|  |  |
| --- | --- |
| **Kegiatan**  **Pembelajaran** | **Deskripsi** |
|  | 1. Peserta didik diberikan stimulus dalam bentuk tayangan video mengenai pengertian dan fungsi   proxy server dalam jaringan. [Video Pengantar Proxy Server](https://youtu.be/QlT5fEPhmBI)   1. Pendidik menjelaskan materi tentang proxy server, fungsinya dalam mengamankan dan mempercepat akses internet, serta jenis-jenis proxy server yang ada. 2. Pendidik memberikan referensi video yang menjelaskan cara kerja dan konfigurasi proxy server:    * [Pengertian dan Jenis Proxy Server](https://youtu.be/LE8AHJacCFM)    * Buku Elektronik Penunjang: [Konfigurasi Proxy Server](https://www.academia.edu/16832625/Pemrograman_web_statis_dan_dinamis) 3. Peserta didik melakukan latihan untuk mengonfigurasi proxy server di jaringan rumah menggunakan software proxy seperti **Squid** atau **Mikrotik**. 4. Peserta didik diminta untuk mendiskusikan penerapan proxy server dalam meningkatkan keamanan dan kontrol akses di jaringan. 5. Peserta didik menyusun dan merangkum langkah-langkah konfigurasi proxy server serta manfaat yang diperoleh dari penggunaannya. 6. Masing-masing kelompok mempresentasikan hasil latihan dan diskusi mereka menggunakan media seperti PowerPoint, video tutorial, atau naskah cerita. 7. Pendidik meminta kelompok lain untuk memberikan tanggapan terhadap presentasi kelompok lainnya. 8. Setiap kelompok mencatat masukan dan memperbaiki presentasi mereka. 9. 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 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.
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 "Pengertian dan Jenis Proxy Server": [Jenis Proxy Server](https://youtu.be/LE8AHJacCFM). Buku Elektronik Penunjang Belajar: [Panduan Proxy Server](https://www.academia.edu/16832625/Pemrograman_web_statis_dan_dinamis).

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.

Daftar Pustaka

1. Dicoding, "Ngoding Web Dinamis Atau Statis", 15 Januari 2020, [dicoding.com](https://www.dicoding.com/blog/ngoding-web-dinamis-atau-statis/).
2. Dewaweb, "Perbedaan Web Statis dan Web Dinamis", 27 Mei 2022, [dewaweb.com](https://dewaweb.com/).
3. Santoso, A. (2019). Pemrograman Web untuk Pemula. Informatika 7 in 1 Pemrograman Web untuk Pemula - Rohi Abdulloh - Google Buku.

## 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. Pendidik memberikan kesempatan kepada beberapa peserta didik untuk membahas materi pertemuan sebelumnya tentang proxy server dan penerapannya. 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 manfaat dari penggunaan proxy server internal?    2. Apa saja konfigurasi dasar yang perlu dilakukan untuk mengaktifkan proxy server 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 cara mengonfigurasi proxy server internal di Mikrotik. [Video Proxy Internal Mikrotik](https://youtu.be/QlT5fEPhmBI) 3. Pendidik menjelaskan materi tentang konfigurasi proxy server internal di Mikrotik, termasuk pengaturan cache, filter konten, dan pengelolaan akses pengguna. 4. Pendidik memberikan referensi video yang menjelaskan cara konfigurasi proxy server internal di Mikrotik:    * [Konfigurasi Proxy Server Mikrotik](https://youtu.be/LE8AHJacCFM)    * Buku Elektronik Penunjang: [Panduan Mikrotik untuk Proxy Server](https://www.academia.edu/16832625/Pemrograman_web_statis_dan_dinamis) 5. Peserta didik melakukan latihan konfigurasi proxy server internal di Mikrotik dengan mengikuti langkah-langkah yang telah diajarkan. 6. Peserta didik diminta untuk mengidentifikasi manfaat penggunaan proxy internal dalam mengamankan dan mengoptimalkan lalu lintas jaringan. 7. Peserta didik mendiskusikan cara-cara mengelola kebijakan akses menggunakan proxy server dan implementasi kontrol konten. 8. Peserta didik menyusun dan merangkum langkah-langkah konfigurasi proxy server di Mikrotik serta manfaat yang diperoleh dari penggunaannya. 9. Masing-masing kelompok mempresentasikan hasil latihan dan diskusi mereka menggunakan |

|  |  |
| --- | --- |
| **Kegiatan**  **Pembelajaran** | **Deskripsi** |
|  | 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 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.
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 "Pengertian dan Konfigurasi Proxy Internal di Mikrotik": [Konfigurasi Proxy Mikrotik](https://youtu.be/LE8AHJacCFM). Buku Elektronik Penunjang Belajar: [Panduan Mikrotik Proxy Server](https://www.academia.edu/16832625/Pemrograman_web_statis_dan_dinamis).

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

Daftar Pustaka

1. Dicoding, "Ngoding Web Dinamis Atau Statis", 15 Januari 2020, [dicoding.com](https://www.dicoding.com/blog/ngoding-web-dinamis-atau-statis/).
2. Dewaweb, "Perbedaan Web Statis dan Web Dinamis", 27 Mei 2022, [dewaweb.com](https://dewaweb.com/).
3. Santoso, A. (2019). Pemrograman Web untuk Pemula. Informatika 7 in 1 Pemrograman Web untuk Pemula - Rohi Abdulloh - Google Buku.

## 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. 4. Masing-masing kelompok mempresentasikan hasil latihan dan diskusi mereka menggunakan media seperti PowerPoint, video tutorial, atau naskah cerita. 5. Pendidik meminta kelompok lain untuk memberikan tanggapan terhadap presentasi kelompok lainnya. 6. Setiap kelompok mencatat masukan dan memperbaiki presentasi mereka. 7. 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 |

|  |  |
| --- | --- |
| **Kegiatan**  **Pembelajaran** | **Deskripsi** |
|  | teman-teman yang masih belum memahami.   1. Guru menjelaskan materi minggu depan dan bahan yang perlu dipersiapkan siswa untuk kelancaran pembelajaran berikutnya. 2. 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? | [ ] | [ ] | [ ] |
| 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.
2. Squid Proxy: Perangkat lunak open-source yang sering digunakan untuk membangun server proxy eksternal. Squid memungkinkan pengelolaan cache, kontrol akses, dan filtering situs web.
3. 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.

Daftar Pustaka

1. Dicoding, "Ngoding Web Dinamis Atau Statis", 15 Januari 2020, [dicoding.com](https://www.dicoding.com/blog/ngoding-web-dinamis-atau-statis/).
2. Dewaweb, "Perbedaan Web Statis dan Web Dinamis", 27 Mei 2022, [dewaweb.com](https://dewaweb.com/).
3. Santoso, A. (2019). Pemrograman Web untuk Pemula. Informatika 7 in 1 Pemrograman Web untuk Pemula - Rohi Abdulloh - Google Buku.

## 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:    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. 9. Pendidik meminta kelompok lain untuk memberikan tanggapan terhadap presentasi kelompok lainnya. 10. Setiap kelompok mencatat masukan dan memperbaiki presentasi mereka. 11. 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? | [ ] | [ ] | [ ] |

|  |  |  |  |
| --- | --- | --- | --- |
| **Pertanyaan Refleksi** | **Baik** | **Cukup** | **Kurang** |
| 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.

Daftar Pustaka

1. Dicoding, "Ngoding Web Dinamis Atau Statis", 15 Januari 2020, [dicoding.com](https://www.dicoding.com/blog/ngoding-web-dinamis-atau-statis/).
2. Dewaweb, "Perbedaan Web Statis dan Web Dinamis", 27 Mei 2022, [dewaweb.com](https://dewaweb.com/).
3. Santoso, A. (2019). Pemrograman Web untuk Pemula. Informatika 7 in 1 Pemrograman Web untuk Pemula - Rohi Abdulloh - Google Buku.

## 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. |

|  |  |
| --- | --- |
| **Kegiatan**  **Pembelajaran** | **Deskripsi** |
|  | 1. Pendidik melakukan presensi. 2. Pendidik memberikan kesempatan kepada beberapa peserta didik untuk membahas materi pertemuan sebelumnya tentang pengaturan kebijakan proxy server. 3. Pendidik bersama dengan peserta didik menyepakati keyakinan kelas yang akan dilaksanakan selama pembelajaran. 4. Pendidik menyampaikan tujuan pembelajaran dan menyepakatinya dengan siswa. 5. 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. 7. Peserta didik menyusun dan merangkum langkah-langkah monitoring lalu lintas jaringan serta manfaatnya untuk pengelolaan jaringan yang lebih baik. 8. Masing-masing kelompok mempresentasikan hasil latihan dan diskusi mereka menggunakan media seperti PowerPoint, video tutorial, atau naskah cerita. 9. Pendidik meminta kelompok lain untuk memberikan tanggapan terhadap presentasi kelompok lainnya. 10. Setiap kelompok mencatat masukan dan memperbaiki presentasi mereka. 11. 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.

Daftar Pustaka

1. Dicoding, "Ngoding Web Dinamis Atau Statis", 15 Januari 2020, [dicoding.com](https://www.dicoding.com/blog/ngoding-web-dinamis-atau-statis/).
2. Dewaweb, "Perbedaan Web Statis dan Web Dinamis", 27 Mei 2022, [dewaweb.com](https://dewaweb.com/).
3. Santoso, A. (2019). Pemrograman Web untuk Pemula. Informatika 7 in 1 Pemrograman Web untuk Pemula - Rohi Abdulloh - Google Buku.

## 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**  **Pembelajaran** | **Deskripsi** |
| **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. 9. Pendidik meminta kelompok lain untuk memberikan tanggapan terhadap presentasi kelompok lainnya. 10. Setiap kelompok mencatat masukan dan memperbaiki presentasi mereka. 11. 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? | [ ] | [ ] | [ ] |
| 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.

Daftar Pustaka

1. Dicoding, "Ngoding Web Dinamis Atau Statis", 15 Januari 2020, [dicoding.com](https://www.dicoding.com/blog/ngoding-web-dinamis-atau-statis/).
2. Dewaweb, "Perbedaan Web Statis dan Web Dinamis", 27 Mei 2022, [dewaweb.com](https://dewaweb.com/).
3. Santoso, A. (2019). Pemrograman Web untuk Pemula. Informatika 7 in 1 Pemrograman Web untuk Pemula - Rohi Abdulloh - Google Buku.

## 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:    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. |

|  |  |
| --- | --- |
| **Kegiatan**  **Pembelajaran** | **Deskripsi** |
|  | 1. 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. 3. Masing-masing kelompok mempresentasikan hasil latihan dan diskusi mereka menggunakan media seperti PowerPoint, video tutorial, atau naskah cerita. 4. Pendidik meminta kelompok lain untuk memberikan tanggapan terhadap presentasi kelompok lainnya. 5. Setiap kelompok mencatat masukan dan memperbaiki presentasi mereka. 6. 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? | [ ] |
| 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.
3. Kerentanan Keamanan: Titik lemah dalam sistem yang dapat dieksploitasi oleh pihak yang tidak sah untuk mengakses atau merusak data dan sistem.
4. Firewall: Alat untuk memfilter dan mengontrol lalu lintas data yang masuk dan keluar dari jaringan untuk melindungi sistem dari serangan eksternal.
5. Proxy Server: Server yang bertindak sebagai perantara antara pengguna dan internet untuk meningkatkan keamanan dan kontrol akses.

Daftar Pustaka

1. Dicoding, "Ngoding Web Dinamis Atau Statis", 15 Januari 2020, [dicoding.com](https://www.dicoding.com/blog/ngoding-web-dinamis-atau-statis/).
2. Dewaweb, "Perbedaan Web Statis dan Web Dinamis", 27 Mei 2022, [dewaweb.com](https://dewaweb.com/).
3. Santoso, A. (2019). Pemrograman Web untuk Pemula. Informatika 7 in 1 Pemrograman Web untuk Pemula - Rohi Abdulloh - Google Buku.

## 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) 3. 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.    * **User Manager** untuk mengatur kebijakan akses dan hak pengguna. 4. 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) 5. 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**. 6. Peserta didik diminta untuk mendiskusikan dan menganalisis implementasi kebijakan keamanan dalam skenario dunia nyata, seperti pada jaringan perusahaan atau sekolah. |

|  |  |
| --- | --- |
| **Kegiatan**  **Pembelajaran** | **Deskripsi** |
|  | 1. Peserta didik menyusun dan merangkum langkah-langkah pengaturan kebijakan keamanan di   Mikrotik serta manfaat yang diperoleh dari penerapannya.   1. Masing-masing kelompok mempresentasikan hasil latihan dan diskusi mereka menggunakan media seperti PowerPoint, video tutorial, atau naskah cerita. 2. Pendidik meminta kelompok lain untuk memberikan tanggapan terhadap presentasi kelompok lainnya. 3. Setiap kelompok mencatat masukan dan memperbaiki presentasi mereka. 4. 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.

Daftar Pustaka

1. Dicoding, "Ngoding Web Dinamis Atau Statis", 15 Januari 2020, [dicoding.com](https://www.dicoding.com/blog/ngoding-web-dinamis-atau-statis/).
2. Dewaweb, "Perbedaan Web Statis dan Web Dinamis", 27 Mei 2022, [dewaweb.com](https://dewaweb.com/).
3. Santoso, A. (2019). Pemrograman Web untuk Pemula. Informatika 7 in 1 Pemrograman Web untuk Pemula - Rohi Abdulloh - Google Buku.

## 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. 9. Masing-masing kelompok mempresentasikan hasil latihan dan diskusi mereka menggunakan media seperti PowerPoint, video tutorial, atau naskah cerita. 10. Pendidik meminta kelompok lain untuk memberikan tanggapan terhadap presentasi kelompok lainnya. 11. Setiap kelompok mencatat masukan dan memperbaiki presentasi mereka. 12. Pendidik meminta kelompok untuk mengumpulkan hasil presentasi yang sudah disempurnakan sesuai media yang dipilih. |

|  |  |
| --- | --- |
| **Kegiatan**  **Pembelajaran** | **Deskripsi** |
| **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.

Daftar Pustaka

1. Dicoding, "Ngoding Web Dinamis Atau Statis", 15 Januari 2020, [dicoding.com](https://www.dicoding.com/blog/ngoding-web-dinamis-atau-statis/).
2. Dewaweb, "Perbedaan Web Statis dan Web Dinamis", 27 Mei 2022, [dewaweb.com](https://dewaweb.com/).
3. Santoso, A. (2019). Pemrograman Web untuk Pemula. Informatika 7 in 1 Pemrograman Web untuk Pemula - Rohi Abdulloh - Google Buku.

## 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. 9. 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? | [ ] | [ ] | [ ] |
| 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.

Daftar Pustaka

1. Dicoding, "Ngoding Web Dinamis Atau Statis", 15 Januari 2020, [dicoding.com](https://www.dicoding.com/blog/ngoding-web-dinamis-atau-statis/).
2. Dewaweb, "Perbedaan Web Statis dan Web Dinamis", 27 Mei 2022, [dewaweb.com](https://dewaweb.com/).
3. Santoso, A. (2019). Pemrograman Web untuk Pemula. Informatika 7 in 1 Pemrograman Web untuk Pemula - Rohi Abdulloh - Google Buku.

## 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:    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. 3. Pendidik mengajak peserta didik untuk membahas solusi dan perbaikan yang dapat diterapkan pada pengelolaan keamanan jaringan di dunia nyata. 4. Peserta didik menyusun kesimpulan mengenai apa yang telah mereka pelajari dan seberapa pentingnya topik-topik tersebut untuk pengelolaan jaringan yang aman. 5. 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. 6. Pendidik memberikan umpan balik terhadap hasil refleksi dan presentasi kelompok. 7. Pendidik memberikan klarifikasi dan memperkuat pemahaman peserta didik mengenai materi yang perlu dipahami lebih dalam. 8. 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? | [ ] |

|  |  |  |
| --- | --- | --- |
| **No** | **Pertanyaan** | **Jawaban** |
| 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.

# INSTRUMEN PENILAIAN

**1.** Asesmen Sumatif

**Mata Pelajaran**: Keamanan Jaringan

**Bentuk Soal**: Pilihan Ganda

**Kelas/Semester**: XII / Genap

**Nama Guru**: Fachry Septian Dinarre, S.Kom

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **No.** | **Tujuan Pembelajaran** | **Materi** | **Indikator Butir Soal** | **Soal** | **Kunci Jawaban** |
| 1 | Memahami konsep  dasar keamanan jaringan | Firewall & Proxy | Menjelaskan pengertian firewall dan proxy | Manakah pernyataan yang benar tentang firewall? | B |
| 2 | Memahami konsep  dasar keamanan jaringan | Firewall | Menjelaskan fungsi firewall | Apa fungsi utama dari firewall dalam jaringan? | A |
| 3 | Mengetahui jenis ancaman jaringan | Ancaman Keamanan Jaringan | Identifikasi jenis ancaman | Manakah yang termasuk jenis serangan DoS (Denial of Service)? | B |
| 4 | Mengkonfigurasi firewall dan proxy pada perangkat Mikrotik | Mikrotik Firewall & Proxy Setup | Praktik konfigurasi firewall dan proxy | Apa langkah pertama dalam mengonfigurasi firewall pada Mikrotik? | C |
| 5 | Memahami implementasi VPN | VPN pada Mikrotik | Menyusun konfigurasi VPN | Manakah yang benar tentang VPN (Virtual Private Network)? | A |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **No.** | **Tujuan Pembelajaran** | **Materi** | **Indikator Butir Soal** | **Soal** | **Kunci Jawaban** |
| 6 | Mengetahui cara mitigasi ancaman menggunakan Mikrotik | Firewall & Mitigasi Ancaman | Implementasi mitigasi ancaman | Apa yang dimaksud dengan mitigasi ancaman pada jaringan? | A |
| 7 | Memahami cara menganalisa dan mengoptimalkan konfigurasi | Analisis Keamanan & Optimasi | Mengoptimalkan konfigurasi firewall dan proxy | Bagaimana cara menganalisa trafik jaringan menggunakan Mikrotik untuk deteksi ancaman? | B |
| 8 | Mengetahui jenis serangan yang dapat terdeteksi | Serangan DDoS dan Port Scanning | Mendeteksi serangan DDoS | Manakah yang merupakan gejala dari serangan DDoS pada jaringan? | A |
| 9 | Mengetahui penerapan kebijakan akses di jaringan | Kontrol Akses  & User Manager | Menyusun kebijakan kontrol akses | Apa peran **User Manager** dalam kontrol akses pada jaringan Mikrotik? | C |
| 10 | Mengetahui tentang pengaturan proxy server | Proxy Server pada Mikrotik & Ubuntu | Mengonfigurasi proxy server | Apa keuntungan utama menggunakan proxy server dalam jaringan? | B |

## Kunci Jawaban dan Skor:

|  |  |  |
| --- | --- | --- |
| **No** | **Kunci** | **Skor** |
| 1 | B | 10 |
| 2 | A | 10 |
| 3 | B | 10 |
| 4 | C | 10 |
| 5 | A | 10 |
| 6 | A | 10 |
| 7 | B | 10 |
| 8 | A | 10 |
| 9 | C | 10 |
| 10 | B | 10 |

Deskripsi Penilaian:

**86-100%** = Sudah mencapai ketuntasan, perlu pengayaan atau tantangan lebih

**66-85%** = Sudah mencapai ketuntasan, tidak perlu ada pembahasan ulang

**41-65%** = Belum mencapai ketuntasan, dijelaskan dan dibahas ulang di bagian yang diperlukan

**0-40%** = Belum mencapai, diulangi lagi untuk pembahasan

Asesmen Formatif

|  |  |  |
| --- | --- | --- |
| **No** | **Indikator** | **Ketercapaian** |
| 1 | Mengetahui konsep dasar keamanan jaringan | Pengertian Firewall, Proxy, VPN |
| 2 | Mengetahui jenis ancaman pada jaringan | Serangan DDoS, Port Scanning, Phishing |
| 3 | Mengonfigurasi dan menganalisa trafik dengan Mikrotik | Pengaturan firewall, proxy, VPN, analisis trafik |

|  |  |  |
| --- | --- | --- |
| **No** | **Indikator** | **Ketercapaian** |
| 4 | Mengimplementasikan kebijakan akses dan kontrol pengguna | Penggunaan **User Manager** pada Mikrotik |

## Rubrik Penilaian:

**Kelas**: XI SIJA

**Tujuan Pembelajaran**: Peserta didik mampu memahami dan mengimplementasikan firewall, proxy, VPN, dan kebijakan kontrol akses jaringan.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Aspek/Dimensi yang Dinilai** | **Kurang (<60)** | **Cukup (61-70)** | **Baik (71-85)** | **Sangat Baik (>85)** |
| **Pemahaman** | Tidak memahami | Memahami dasar- | Memahami dan | Memahami dan mampu |
| **Konsep**  **Keamanan** | konsep dasar firewall, proxy, dan | dasar keamanan jaringan tetapi belum | dapat menjelaskan konsep-konsep | menjelaskan dengan baik serta mengimplementasikan |
| **Jaringan** | VPN | sepenuhnya | dasar serta | konsep secara efektif |
|  |  | menerapkan | penerapannya |  |
| **Kemampuan** | Tidak bisa | Bisa mengonfigurasi | Mengonfigurasi | Mengonfigurasi firewall dan |
| **Mengonfigurasi Firewall & Proxy** | mengonfigurasi firewall atau proxy | firewall dan proxy dengan bimbingan | firewall dan proxy dengan sedikit | proxy dengan sangat baik dan minim kesalahan |
|  |  |  | kesalahan |  |
| **Deteksi dan** | Tidak bisa | Bisa mendeteksi | Dapat mendeteksi | Dapat mendeteksi dan |
| **Mitigasi Ancaman** | mendeteksi dan | ancaman, tetapi | dan memitigasi | memitigasi ancaman secara |
|  | memitigasi ancaman | mitigasi belum optimal | ancaman dengan baik | tepat dan efektif |
| **Kebijakan Akses** | Tidak bisa | Menyusun kebijakan | Menyusun kebijakan | Menyusun kebijakan akses |
| **dan Pengelolaan** | menyusun | akses dasar tetapi | akses yang lebih | dan kontrol pengguna |
| **User** | kebijakan akses | belum efektif | baik dan hampir | dengan sangat baik dan |
|  | dan kontrol user |  | efektif | optimal |

### Deskripsi Penilaian:

Penilaian ini bertujuan untuk mengevaluasi pemahaman dan keterampilan peserta didik dalam mengonfigurasi dan mengimplementasikan solusi keamanan jaringan seperti firewall dan proxy, serta bagaimana mereka mengelola dan mengamankan jaringan melalui kebijakan akses yang sesuai.

Aspek/Dimensi yang Dinilai

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Aspek/Dimensi** | **Kurang (<60)** | **Cukup (61-70)** | **Baik (71-85)** | **Sangat Baik (>85)** |
| **Pemahaman** | Tidak memahami | Memahami dasar-dasar | Memahami dan dapat | Memahami konsep |
| **Konsep** | konsep dasar | keamanan jaringan | menjelaskan dengan | secara mendalam dan |
| **Keamanan** | keamanan | tetapi belum | baik konsep dasar | mampu menjelaskan |
| **Jaringan** | jaringan (firewall, | sepenuhnya mampu | keamanan jaringan | serta |
|  | proxy, VPN). Tidak dapat | menjelaskan penerapannya. | serta penerapannya. | mengimplementasikan penerapannya dengan |
|  | menjelaskan |  |  | baik. |
|  | penerapannya. |  |  |  |
| **Kemampuan** | Tidak bisa | Bisa mengonfigurasi | Mengonfigurasi firewall | Mengonfigurasi firewall |
| **Mengonfigurasi Firewall & Proxy** | mengonfigurasi firewall atau | firewall dan proxy dengan bantuan atau | dan proxy dengan sedikit kesalahan dan | dan proxy dengan sangat baik, minim |
|  | proxy. Tidak dapat | bimbingan, masih | membutuhkan sedikit | kesalahan, dan dapat |
|  | membuat | sering keliru. | bimbingan. | mengonfigurasi berbagai |
|  | pengaturan dasar |  |  | fitur dengan efisien. |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Aspek/Dimensi** | **Kurang (<60)** | **Cukup (61-70)** | **Baik (71-85)** | **Sangat Baik (>85)** |
|  | pada Mikrotik atau  Ubuntu. |  |  |  |
| **Deteksi dan** | Tidak bisa | Bisa mendeteksi | Mendeteksi ancaman | Dapat mendeteksi |
| **Mitigasi Ancaman** | mendeteksi atau memitigasi | ancaman, tetapi tidak optimal dalam | dengan baik dan mampu memitigasi | ancaman dengan tepat dan mitigasi ancaman |
|  | ancaman pada | mengimplementasikan | sebagian besar | dilakukan secara tepat, |
|  | jaringan, tidak | mitigasi. | ancaman yang | efektif, dan efisien. |
|  | tahu cara |  | ditemukan. |  |
|  | mengidentifikasi serangan. |  |  |  |
| **Kebijakan Akses** | Tidak bisa | Menyusun kebijakan | Menyusun kebijakan | Menyusun kebijakan |
| **dan Pengelolaan** | menyusun | akses dasar tetapi | akses dengan baik, dan | akses dan kontrol |
| **User** | kebijakan akses | belum efektif, masih | mengimplementasikan | pengguna dengan |
|  | dan kontrol pengguna, tidak | membutuhkan bimbingan dalam | **User Manager** untuk kontrol akses yang lebih | sangat baik, menggunakan **User** |
|  | tahu cara | implementasi. | efektif. | **Manager** secara efektif, |
|  | menggunakan |  |  | dan mampu mengelola |
|  | **User Manager**. |  |  | pengguna dengan efisien. |
| **Kemampuan Mengidentifikasi** | Tidak dapat mengidentifikasi | Bisa mengidentifikasi masalah dengan | Mampu mengidentifikasi masalah dengan cukup | Dapat mengidentifikasi masalah secara cepat |
| **dan** | masalah pada | bimbingan, namun | cepat dan | dan menyelesaikan |
| **Menyelesaikan** | konfigurasi | belum bisa | menyelesaikan | masalah dengan tepat |
| **Masalah** | firewall atau | menyelesaikan masalah | sebagian besar | serta menemukan solusi |
|  | proxy, serta tidak tahu cara | secara mandiri. | masalah secara mandiri. | terbaik dengan sedikit atau tanpa bantuan. |
|  | memperbaikinya. |  |  |  |

Deskripsi Penilaian:

**Kurang (<60)**: Peserta didik belum mencapai pemahaman atau keterampilan yang diharapkan. Membutuhkan pengulangan materi dan bimbingan lebih lanjut.

**Cukup (61-70)**: Peserta didik sudah mulai memahami konsep dan dapat mengimplementasikan sebagian besar materi, namun masih membutuhkan bimbingan lebih lanjut dalam beberapa area.

**Baik (71-85)**: Peserta didik dapat mengimplementasikan materi dengan cukup baik dan hampir dapat bekerja mandiri dalam mengonfigurasi firewall, proxy, dan kebijakan akses.

**Sangat Baik (>85)**: Peserta didik menguasai materi dengan baik dan dapat mengimplementasikan konsep-konsep tersebut secara mandiri serta efektif. Peserta didik juga mampu mengidentifikasi dan memecahkan masalah terkait pengelolaan keamanan jaringan.

## Skala Penilaian:

|  |  |
| --- | --- |
| **Skor** | **Deskripsi** |
| **91-100** | Sangat baik, penguasaan materi dan keterampilan sangat baik, dapat bekerja secara mandiri dan efisien. |
| **76-90** | Baik, penguasaan materi sudah cukup baik, dapat bekerja dengan sedikit bantuan dan hampir mandiri. |
| **60-75** | Cukup, masih membutuhkan bimbingan lebih lanjut dalam penerapan konsep-konsep yang telah dipelajari. |
| **<60** | Kurang, perlu pengulangan materi dan latihan lebih lanjut dalam penerapan keterampilan yang dipelajari. |

Penilaian Sikap: Keamanan Jaringan

Penilaian sikap adalah bagian penting dalam evaluasi peserta didik, yang tidak hanya mencakup penguasaan materi, tetapi juga mencakup sikap, perilaku, dan keterampilan dalam berinteraksi, bekerja sama, serta menerapkan nilai-nilai yang sesuai dengan pembelajaran yang dilakukan. Berikut adalah **penilaian sikap** yang dirancang untuk materi **Keamanan Jaringan**.

## Aspek yang Dinilai dalam Penilaian Sikap:

### Sikap Terhadap Pembelajaran

**Kriteria**: Peserta didik menunjukkan **antusiasme**, **kesungguhan**, dan **keterlibatan aktif** selama pembelajaran. Mereka berusaha untuk selalu **terlibat dalam diskusi**, menyelesaikan tugas dengan baik, serta siap untuk mempelajari materi yang lebih sulit.

### Sikap Terhadap Kerja Sama

**Kriteria**: Peserta didik mampu bekerja dalam **kelompok** dengan **baik**, saling menghargai pendapat teman, **berkolaborasi dalam menyelesaikan tugas** praktikum (misalnya, konfigurasi firewall dan proxy), dan **memberikan masukan konstruktif** kepada kelompok lain.

### Sikap Terhadap Tanggung Jawab

**Kriteria**: Peserta didik menunjukkan **rasa tanggung jawab** terhadap tugas yang diberikan, baik dalam

**menyelesaikan latihan** secara mandiri maupun dalam **kerja kelompok**. Mereka **bertanggung jawab terhadap keberhasilan pembelajaran** mereka sendiri dan teman-temannya.

### Sikap Terhadap Keamanan Data dan Privasi

**Kriteria**: Peserta didik menunjukkan **kesadaran tinggi terhadap pentingnya keamanan data** dan **privasi**. Mereka memahami dan **menghargai etika dalam mengelola data** pribadi serta informasi yang ada dalam jaringan yang mereka kelola.

### Sikap Terhadap Penerapan Prinsip Etika

**Kriteria**: Peserta didik menunjukkan **integritas** dan **etika yang tinggi** dalam praktik keamanan jaringan. Mereka memahami pentingnya **menjaga kerahasiaan informasi** dan **menghindari tindakan yang dapat merugikan orang lain** (misalnya, melakukan hacking atau akses tidak sah ke jaringan).

Rubrik Penilaian Sikap

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Aspek yang Dinilai** | **Sangat Baik (4)** | **Baik (3)** | **Cukup (2)** | **Kurang (1)** |
| **Sikap Terhadap Pembelajaran** | Selalu aktif, sangat antusias, selalu mengajukan pertanyaan dan menyelesaikan tugas tepat waktu. | Aktif dan berpartisipasi dalam diskusi, menyelesaikan tugas dengan baik. | Sesekali aktif, hanya menyelesaikan tugas tanpa inisiatif lebih. | Tidak aktif, jarang berpartisipasi dalam diskusi, dan tugas sering tertunda. |
| **Sikap Terhadap Kerja Sama** | Selalu menghargai teman, bekerja sama dengan baik, berkontribusi dalam diskusi kelompok. | Berkolaborasi dengan baik, menghargai pendapat teman. | Kadang-kadang sulit berkolaborasi, namun dapat menyelesaikan tugas kelompok. | Tidak berusaha bekerja sama, sulit menerima kritik atau saran dari teman. |
| **Sikap Terhadap Tanggung Jawab** | Menyelesaikan tugas dengan penuh tanggung jawab dan tidak perlu diingatkan. | Menyelesaikan tugas dengan baik dan tepat waktu. | Tugas selesai tetapi tidak sepenuhnya optimal atau terlambat. | Tidak menyelesaikan tugas tepat waktu, sering mengabaikan tanggung jawab. |
| **Sikap Terhadap Keamanan Data dan Privasi** | Selalu menjaga data pribadi dan privasi, paham pentingnya enkripsi dan perlindungan data. | Memahami pentingnya keamanan dan privasi, tetapi terkadang tidak sepenuhnya berhati- hati. | Mengetahui tentang keamanan data, namun kurang konsisten dalam menerapkannya. | Kurang memahami pentingnya privasi dan keamanan data, sering mengabaikan perlindungan informasi. |
| **Sikap Terhadap Penerapan**  **Prinsip Etika** | Selalu bertindak dengan etika tinggi, tidak pernah | Biasanya bertindak dengan etika, tetapi kadang kurang hati- | Mengetahui etika, namun sering tidak | Tidak mengikuti prinsip etika dalam keamanan |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Aspek yang Dinilai** | **Sangat Baik (4)** | **Baik (3)** | **Cukup (2)** | **Kurang (1)** |
|  | melakukan tindakan  yang merugikan orang lain. | hati dalam beberapa  situasi. | memperhatikan dalam  beberapa kasus. | jaringan, sering  bertindak sembarangan. |

Skala Penilaian Sikap:

|  |  |
| --- | --- |
| **Skor** | **Deskripsi** |
| **16-**  **20** | **Sangat Baik**: Peserta didik menunjukkan sikap yang sangat baik, memiliki etika yang kuat dan bekerja dengan penuh tanggung jawab. |
| **11-15** | **Baik**: Peserta didik memiliki sikap yang baik, namun masih perlu perbaikan pada beberapa aspek. |
| **6-10** | **Cukup**: Peserta didik masih perlu bimbingan dalam menunjukkan sikap yang lebih baik dalam pembelajaran dan kerja sama. |
| **1-5** | **Kurang**: Peserta didik belum menunjukkan sikap yang sesuai dengan harapan dalam pembelajaran, kerjasama, dan tanggung jawab. |

Deskripsi Penilaian Sikap:

**16-20**: Peserta didik sangat aktif dan bertanggung jawab. Mereka memiliki sikap yang sangat baik dalam bekerja sama, menjaga etika, dan mematuhi prinsip-prinsip keamanan data dan privasi. Mereka menjadi contoh yang baik bagi teman- temannya.

**11-15**: Peserta didik aktif dan menunjukkan sikap baik dalam bekerja sama dan bertanggung jawab. Namun, masih ada beberapa area yang perlu diperbaiki untuk mencapai tingkat sikap yang sangat baik.

**6-10**: Peserta didik perlu lebih banyak perhatian dan bimbingan untuk memperbaiki sikap, baik dalam bekerja sama, mengikuti prinsip etika, maupun dalam menyelesaikan tugas dengan lebih tanggung jawab.

**1-5**: Peserta didik membutuhkan banyak perbaikan dalam sikap. Mereka sering kurang aktif, tidak bertanggung jawab, dan sering mengabaikan prinsip etika dalam pembelajaran dan praktik. Pendekatan yang lebih intensif dibutuhkan untuk membantu mereka berkembang.

PENILAIAN SIKAP

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **No** | **Nama Siswa** | **Mandiri** | **Bergotong Royong** | **Bernalar Kritis** | **Berkebhinekaan Global** | **Kreatif** | **Nilai Akhir** |
|  |  | 1 | 2 | 3 | 4 | 1 | 2 |
| 1. |  |  |  |  |  |  |  |
| 2. |  |  |  |  |  |  |  |
| 3. |  |  |  |  |  |  |  |
| 4. |  |  |  |  |  |  |  |
| 5. |  |  |  |  |  |  |  |
| 6. |  |  |  |  |  |  |  |
| 7. |  |  |  |  |  |  |  |
| 8. |  |  |  |  |  |  |  |
| 9. |  |  |  |  |  |  |  |
| 10. |  |  |  |  |  |  |  |

Rubrik Penilaian Sikap Profil Pelajar Pancasila

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Aspek yang Dinilai** | **Skor 4 (Sangat Baik)** | **Skor 3 (Baik)** | **Skor 2 (Cukup)** | **Skor 1 (Kurang)** |
| **Mandiri** | Peserta didik selalu | Peserta didik sering | Peserta didik | Peserta didik |
|  | bekerja dengan inisiatif, | menyelesaikan tugas | terkadang | bergantung pada |
|  | dapat menyelesaikan | secara mandiri, | membutuhkan | bantuan orang lain |
|  | tugas tanpa bantuan, dan selalu menunjukkan | meskipun kadang membutuhkan sedikit | bimbingan lebih intensif, dan kurang | untuk menyelesaikan tugas, tidak mampu |
|  | kemandirian dalam | bimbingan atau | mandiri dalam | bekerja mandiri. |
|  | tugas praktikum dan | bantuan. | menyelesaikan tugas. |  |
|  | teori. |  |  |  |
| **Bergotong Royong** | Peserta didik selalu aktif dalam bekerja sama, | Peserta didik bekerja sama dengan baik, | Peserta didik kadang- kadang kurang | Peserta didik tidak aktif bekerja sama dan tidak |
|  | menghargai pendapat | meskipun terkadang | berkolaborasi, dan | dapat berkolaborasi |
|  | teman, dan membantu | membutuhkan sedikit | terkadang tidak | dengan baik dalam |
|  | anggota kelompok | dorongan atau motivasi. | berpartisipasi aktif | kelompok. |
|  | dalam menyelesaikan tugas. |  | dalam diskusi kelompok. |  |
| **Bernalar Kritis** | Peserta didik selalu | Peserta didik dapat | Peserta didik berpikir | Peserta didik kesulitan |
|  | menganalisis masalah | berpikir kritis dan | secara logis, tetapi | dalam berpikir kritis, |
|  | secara mendalam, | menganalisis masalah | kadang kurang | tidak mampu |
|  | mampu mempertimbangkan | dengan cukup baik, namun terkadang tidak | mendalam dalam menganalisis | menganalisis masalah dengan baik dan |
|  | berbagai aspek | mempertimbangkan | masalah atau | membutuhkan banyak |
|  | sebelum mengambil | semua kemungkinan. | kesulitan memahami | bimbingan. |
|  | keputusan. |  | isu kompleks. |  |
| **Berkebhinekaan Global** | Peserta didik sangat menghargai | Peserta didik menghargai | Peserta didik sadar akan keberagaman | Peserta didik kurang menghargai |
|  | keberagaman dan | keberagaman, tetapi | tetapi belum | keberagaman dan |
|  | menunjukkan sikap | kadang-kadang kurang | sepenuhnya | cenderung tidak |
|  | inklusif dalam diskusi | aktif dalam | memahami atau | mempertimbangkan |
|  | dan kerja kelompok, mengapresiasi | mengapresiasi pandangan yang | menerapkan nilai- nilai tersebut dalam | perspektif lain dalam diskusi. |
|  | perspektif yang berbeda. | berbeda. | pembelajaran. |  |
| **Kreatif** | Peserta didik sangat | Peserta didik | Peserta didik kadang- | Peserta didik jarang |
|  | kreatif dalam | menunjukkan | kadang | menunjukkan |
|  | menyelesaikan tugas dan mampu | kreativitas dalam beberapa tugas dan | menunjukkan kreativitas, tetapi | kreativitas dalam tugas atau praktikum dan |
|  | memberikan solusi | dapat memberikan | lebih sering | cenderung hanya |
|  | inovatif pada masalah | solusi yang baik | mengikuti instruksi | mengikuti instruksi |
|  | yang dihadapi. | meskipun tidak terlalu inovatif. | dan tidak mengembangkan ide | tanpa ide baru. |
|  |  |  | baru. |  |

Panduan Penilaian:

**4**: Jika **empat indikator** (dari aspek tersebut) terlihat jelas dalam sikap peserta didik.

**3**: Jika **tiga indikator** terlihat dalam sikap peserta didik. **2**: Jika **dua indikator** terlihat dalam sikap peserta didik. **1**: Jika **satu indikator** terlihat dalam sikap peserta didik.

## Penilaian Nilai Akhir**:**

Nilai akhir akan dihitung berdasarkan skor dari masing-masing aspek yang dinilai. Nilai akhir dapat diberikan dengan menggunakan skala sebagai berikut:

**Skor 16-20**: **Sangat Baik** – Peserta didik menunjukkan sikap yang sangat baik dalam semua aspek.

**Skor 11-15**: **Baik** – Peserta didik menunjukkan sikap yang baik, namun masih dapat diperbaiki dalam beberapa aspek.

**Skor 6-10**: **Cukup** – Peserta didik menunjukkan sikap yang cukup, namun masih perlu bimbingan lebih lanjut.

**Skor 1-5**: **Kurang** – Peserta didik perlu perbaikan signifikan dalam sikap dan kerja sama selama pembelajaran.

Berdasarkan penilaian sikap, peserta didik yang mendapatkan skor rendah pada salah satu aspek dapat diberikan **pendampingan lebih lanjut** dan **bimbingan personal** untuk membantu mereka memperbaiki sikap mereka dalam **kerja sama**, **tanggung jawab**, dan **pengelolaan data pribadi**. Sedangkan peserta didik dengan skor tinggi bisa diberikan **tantangan lebih** dan **peran kepemimpinan** dalam diskusi kelompok atau proyek.

## Rencana Tindak Lanjut**:**

**Materi**: Pengelolaan Keamanan Jaringan

**Kelas/Semester**: XII / Genap

**Capaian Pembelajaran**: Peserta didik mampu mengimplementasikan dan mengelola keamanan jaringan dengan menggunakan firewall, proxy, VPN, serta kebijakan kontrol akses untuk menjaga integritas dan keamanan jaringan.

## Rencana Tindak Lanjut Penilaian Keamanan Jaringan

Rencana tindak lanjut ini bertujuan untuk memberikan bimbingan atau tindakan yang diperlukan berdasarkan hasil penilaian, baik penilaian **pengetahuan**, **keterampilan**, maupun **sikap**. Rencana tindak lanjut disesuaikan dengan hasil penilaian peserta didik untuk membantu mereka mencapai tujuan pembelajaran yang optimal.

## Penilaian Pengetahuan (Asesmen Sumatif)

Rencana Tindak Lanjut Berdasarkan Skor**:**

### Skor 86-100% (Sangat Baik): Tindak Lanjut:

Peserta didik yang memperoleh skor tinggi menunjukkan penguasaan materi yang baik.

Diberikan **tantangan lebih** berupa **studi kasus lanjutan**, atau **proyek independen** untuk mengimplementasikan pengetahuan lebih mendalam, seperti menganalisis jaringan besar atau mengonfigurasi **firewall dan proxy dalam skenario dunia nyata**.

Diberikan kesempatan untuk **berkolaborasi sebagai mentor** bagi peserta didik lain yang membutuhkan bantuan.

### Skor 66-85% (Baik): Tindak Lanjut:

Peserta didik yang memperoleh skor baik sudah memahami materi dasar dengan cukup baik, tetapi perlu sedikit penguatan dalam beberapa topik.

**Review materi** untuk konsep-konsep yang belum sepenuhnya dipahami (misalnya, perbedaan antara firewall stateful dan stateless, atau cara pengaturan proxy).

Diberikan **latihan tambahan** dalam bentuk tugas atau simulasi lebih lanjut, serta **diskusi kelompok** untuk memperdalam pemahaman.

### Skor 41-65% (Cukup): Tindak Lanjut:

Peserta didik yang memperoleh skor cukup menunjukkan pemahaman yang terbatas.

**Pemberian bimbingan tambahan** melalui **kelas remedi** atau **pengulangan materi** untuk memperjelas bagian-bagian yang sulit dipahami, seperti **analisis ancaman** atau **konfigurasi firewall**.

Peserta didik diminta untuk mengikuti **tutorial video** dan **membaca materi lebih lanjut** untuk memperkuat pemahaman praktis dan teori.

### Skor 0-40% (Kurang): Tindak Lanjut:

Peserta didik yang mendapatkan skor rendah membutuhkan **pendampingan intensif** dan **bimbingan personal**.

Diadakan **kelas pemulihan** untuk mengulang materi dasar yang belum dipahami.

**Pembagian tugas ringan** untuk mengurangi rasa cemas dan membangun kepercayaan diri mereka, serta

**pemantauan lebih lanjut** selama praktik agar dapat mengevaluasi pemahaman secara lebih intensif.

## Penilaian Keterampilan (Praktek Firewall & Proxy)

Rencana Tindak Lanjut Berdasarkan Hasil Keterampilan**:**

### Skor 86-100% (Sangat Baik): Tindak Lanjut:

Peserta didik yang memperoleh skor tinggi dapat diberikan **proyek lanjutan** dengan konfigurasi lebih kompleks, seperti **pengaturan VPN** atau **analisis lalu lintas jaringan** dengan **tools monitoring**.

Diberikan kesempatan untuk **menyusun panduan atau tutorial** untuk teman sekelas mengenai **best practices** dalam pengelolaan keamanan jaringan.

### Skor 66-85% (Baik): Tindak Lanjut:

Peserta didik yang mendapatkan skor baik dapat diberi **tugas tambahan** untuk memperbaiki bagian yang masih kurang baik, misalnya **optimasi konfigurasi firewall** atau **penyesuaian aturan proxy** untuk skenario tertentu.

Mengadakan **sesi diskusi lebih mendalam** untuk mengidentifikasi kesulitan dan **membantu mereka mengatasi hambatan** yang ada dalam konfigurasi.

### Skor 41-65% (Cukup): Tindak Lanjut:

Peserta didik yang memperoleh skor cukup akan diberi **pendampingan lebih intensif** untuk memperbaiki kesalahan dalam konfigurasi.

Fokus pada **latihan pengaturan dasar**, seperti pembuatan **firewall rules**, **konfigurasi dasar proxy**, dan

### deteksi ancaman sederhana.

Disarankan untuk mengikuti **latihan praktek tambahan** di luar jam pelajaran untuk meningkatkan kemampuan teknis mereka.

### Skor 0-40% (Kurang): Tindak Lanjut:

Peserta didik yang mendapatkan skor rendah perlu **pengulangan materi secara mendalam** dan

**pendampingan individu** dalam latihan konfigurasi dasar.

Penggunaan **simulasi jaringan virtual** atau **lab keamanan** untuk memberikan kesempatan berlatih dengan

**skenario praktis** yang lebih sederhana.

Menerapkan **latihan berulang** dalam pengaturan firewall dan proxy, serta **pemantauan langsung** selama praktik.

## Penilaian Sikap

Rencana Tindak Lanjut Berdasarkan Hasil Penilaian Sikap**:**

### Skor 16-20 (Sangat Baik): Tindak Lanjut:

Peserta didik dengan skor sangat baik dapat **diberikan peran kepemimpinan** dalam diskusi kelompok atau proyek-proyek lanjutan.

Diberikan **tantangan lebih**, seperti **mengembangkan kebijakan keamanan jaringan** untuk organisasi fiktif, atau **mentoring** bagi peserta didik lain yang membutuhkan bantuan.

### Skor 11-15 (Baik): Tindak Lanjut:

Peserta didik yang memperoleh skor baik dapat diberi **tantangan tambahan** untuk lebih **mengembangkan sikap kreatif** dan **berpikir kritis** dalam menyelesaikan masalah jaringan.

Peserta didik yang sedikit kurang terlibat dalam **kerja sama** dapat diberikan lebih banyak kesempatan untuk

**berkolaborasi dalam proyek** dengan anggota kelompok yang lebih aktif.

### Skor 6-10 (Cukup): Tindak Lanjut:

Peserta didik yang mendapat skor cukup perlu **pendampingan intensif** untuk memperbaiki sikap dalam hal

### kerja sama dan tanggung jawab.

Memberikan **pembinaan lebih intensif** dalam hal **etika dan kepemimpinan** selama kerja kelompok, serta

**diskusi kelas** untuk mengembangkan **sikap kritis** terhadap masalah keamanan yang ada.

### Skor 1-5 (Kurang): Tindak Lanjut:

Peserta didik dengan skor rendah perlu mendapatkan **pendampingan lebih intensif** dalam hal **etika**, **tanggung jawab**, dan **kolaborasi tim**.

Diadakan **bimbingan pribadi** untuk meningkatkan **kepercayaan diri** dan **kemampuan berpikir kritis** dalam tugas-tugas praktikum.

Menyusun **strategi peningkatan sikap** dengan melibatkan peserta didik dalam **simulasi peran**, untuk meningkatkan pemahaman tentang pentingnya etika dan kerja tim dalam dunia profesional.

Rencana tindak lanjut ini bertujuan untuk membantu peserta didik mengatasi kesulitan yang mereka hadapi dalam **pemahaman teori**, **praktik teknis**, dan **sikap yang diperlukan** dalam **keamanan jaringan**. Pendekatan diferensiasi berdasarkan hasil penilaian akan memastikan bahwa setiap peserta didik mendapat **dukungan yang sesuai** dengan kemajuan dan kebutuhan mereka.

## 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.

## 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.