Laboratorium
Multimedia dan Internet of Things
Departemen Teknik Komputer
Institut Teknologi Sepuluh Nopember

Laporan Sementara
Praktikum Jaringan Komputer

VPN & QoS

Devanka Raditanti Citasevi - 5024231053

2025

1 Pendahuluan

1.1 Latar Belakang

Dalam era digital yang semakin berkembang pesat, jaringan komputer telah menjadi tulang punggung hampir seluruh aktivitas bisnis dan komunikasi modern. Organisasi, institusi pendidikan, dan perusahaan mengandalkan infrastruktur jaringan untuk berbagi informasi, mengakses sumber daya, dan menjalankan operasional sehari-hari. Ketergantungan yang tinggi terhadap teknologi jaringan ini membawa konsekuensi pada meningkatnya risiko keamanan siber yang dapat mengancam kontinuitas bisnis dan kerahasiaan data. Ancaman keamanan jaringan telah berevolusi menjadi lebih kompleks dan sophisticated, mulai dari serangan malware, intrusi tidak sah, pencurian data, hingga berbagai bentuk cyber attack yang dapat mengakibatkan kerugian finansial dan reputasi yang sangat besar. Perkembangan teknologi digital yang pesat juga diikuti dengan meningkatnya kreativitas para penyerang dalam mengeksploitasi kerentanan sistem jaringan. Oleh karena itu, implementasi sistem keamanan jaringan yang robust dan efektif menjadi kebutuhan yang tidak dapat ditawar-tawar lagi bagi setiap organisasi yang bergantung pada infrastruktur teknologi informasi. Firewall merupakan salah satu komponen fundamental dalam arsitektur keamanan jaringan yang berfungsi sebagai barrier pertama untuk melindungi jaringan internal dari ancaman eksternal. Sebagai mekanisme pertahanan utama, firewall berperan penting dalam mengizinkan lalu lintas jaringan yang dianggap aman untuk melaluinya dan mencegah lalu lintas jaringan yang berpotensi membahayakan. Implementasi firewall yang tepat dan terstruktur dapat secara signifikan mengurangi risiko keamanan dan memberikan kontrol granular terhadap lalu lintas jaringan yang masuk dan keluar dari sistem. Dalam konteks pendidikan jaringan komputer, pemahaman teoritis saja tidak cukup untuk mempersiapkan mahasiswa menghadapi tantangan dunia kerja yang sesungguhnya. Diperlukan pembelajaran praktis yang memberikan pengalaman langsung dalam mengkonfigurasi, mengelola, dan memecahkan masalah keamanan jaringan secara real-time. Modul praktikum ini dirancang khusus untuk menjembatani kesenjangan antara teori dan aplikasi praktis dalam implementasi firewall dan routing, sehingga mahasiswa dapat memperoleh keterampilan hands-on yang sangat dibutuhkan di industri. Keterampilan dalam konfigurasi firewall dan routing merupakan kompetensi yang sangat dibutuhkan dan dicari di industri IT modern. Network administrator, system administrator, dan cybersecurity specialist harus memiliki kemampuan praktis dalam mengimplementasikan dan mengelola sistem keamanan jaringan dengan berbagai tingkat kompleksitas. Modul praktikum ini memberikan fondasi yang kuat untuk pengembangan keterampilan tersebut, sekaligus mempersiapkan mahasiswa untuk menghadapi tantangan keamanan jaringan yang terus berkembang di masa depan.

1.2 Dasar Teori

Firewall adalah sistem keamanan jaringan yang memonitor dan mengontrol lalu lintas jaringan berdasarkan aturan keamanan yang telah ditentukan sebelumnya oleh administrator sistem. Firewall beroperasi sebagai penghalang antara jaringan internal yang terpercaya dengan jaringan eksternal yang tidak terpercaya, seperti internet. Konsep dasar firewall dibangun atas prinsip bahwa semua lalu lintas jaringan harus melewati titik kontrol terpusat yang dapat memfilter, memonitor, dan mengontrol komunikasi berdasarkan kebijakan keamanan yang telah ditetapkan. Fungsi utama firewall mencakup packet filtering yang menyaring paket data berdasarkan alamat IP, port, dan protokol komunikasi. Selain itu, firewall modern juga dilengkapi dengan stateful inspection yang memantau status koneksi dan

memastikan hanya koneksi yang valid dan legitimate yang diizinkan untuk melewati sistem. Application layer filtering merupakan fitur lanjutan yang menganalisis konten aplikasi untuk deteksi ancaman yang lebih sophisticated dan targeted. Network Address Translation (NAT) juga menjadi fungsi penting firewall dalam menyembunyikan struktur jaringan internal dari dunia luar, sehingga memberikan lapisan keamanan tambahan melalui obscurity. IPTables merupakan user-space utility yang memungkinkan administrator sistem untuk mengkonfigurasi tabel yang disediakan oleh Linux kernel firewall. Implementasi IPTables didasarkan pada modul kernel yang terpisah dan menyediakan interface yang powerful untuk mengelola aturan firewall. Arsitektur IPTables dibangun atas konsep tables, chains, rules, dan targets yang bekerja secara hierarkis untuk memproses setiap paket yang melewati sistem. Tables merupakan struktur data yang berisi chain, sementara chains adalah kumpulan rules yang dijalankan secara berurutan. Rules adalah aturan spesifik yang menentukan tindakan terhadap paket, dan targets adalah tindakan yang diambil ketika paket cocok dengan rule tertentu. Tabel utama dalam IPTables mencakup filter table yang merupakan default table untuk packet filtering dengan chains INPUT, OUTPUT, dan FORWARD. Filter table digunakan untuk memutuskan apakah paket diizinkan atau ditolak berdasarkan kriteria yang telah ditetapkan. NAT table digunakan khusus untuk Network Address Translation dengan chains PREROUTING, OUTPUT, dan POSTROUTING yang mengubah alamat sumber atau tujuan paket sesuai kebutuhan. Mangle table digunakan untuk modifikasi header paket dengan chains PREROUTING, OUTPUT, INPUT, FORWARD, dan POSTROUTING yang dapat mengubah quality of service bits, TTL, dan parameter header lainnya. Raw table digunakan untuk konfigurasi exemptions dari connection tracking dengan chains PREROUTING dan OUTPUT. Routing adalah proses fundamental dalam jaringan komputer yang menentukan jalur terbaik untuk mengirimkan paket data dari sumber ke tujuan melalui internetwork. Router menggunakan routing table untuk membuat keputusan forwarding yang optimal berdasarkan alamat tujuan paket dan berbagai parameter jaringan lainnya. Konsep routing mencakup static routing dimana route dikonfigurasi secara manual oleh administrator, dynamic routing dimana route dipelajari melalui routing protocol secara otomatis, dan default routing yang merupakan route yang digunakan ketika tidak ada route spesifik yang tersedia untuk tujuan tertentu. Routing table berisi informasi komprehensif tentang destination network yang merupakan jaringan tujuan, subnet mask untuk menentukan network portion dari alamat IP, gateway atau next hop yang menunjukkan router berikutnya dalam jalur pengiriman paket, interface yang merupakan interface output untuk paket, dan metric yang menunjukkan biaya atau prioritas route. Informasi dalam routing table ini digunakan oleh router untuk membuat keputusan forwarding yang efisien dan optimal. Subnetting adalah proses pembagian network yang besar menjadi subnetwork yang lebih kecil dengan tujuan meningkatkan efisiensi penggunaan alamat IP, mengurangi broadcast domain, meningkatkan keamanan jaringan, dan memudahkan administrasi jaringan. Variable Length Subnet Masking (VLSM) merupakan teknik lanjutan yang memungkinkan penggunaan subnet mask yang berbeda-beda dalam satu network yang sama, sehingga memberikan fleksibilitas dalam alokasi alamat IP sesuai kebutuhan spesifik setiap subnet. Network Address Translation (NAT) adalah teknik yang digunakan untuk memodifikasi informasi alamat IP dalam header paket saat paket transit melalui router atau firewall. NAT memungkinkan multiple device dalam jaringan privat untuk berbagi satu alamat IP publik, sehingga mengatasi keterbatasan alamat IPv4 dan memberikan lapisan keamanan tambahan. Jenis-jenis NAT mencakup Static NAT dengan one-to-one mapping antara alamat privat dan publik, Dynamic NAT dengan pool alamat IP publik yang dialokasikan secara dinamis, dan Port Address Translation (PAT) dengan many-to-one mapping menggunakan port number. Defense in Depth merupakan strategi keamanan berlapis yang mengimplementasikan

multiple layer security controls untuk memberikan perlindungan komprehensif. Strategi ini mencakup perimeter security dengan firewall dan IDS/IPS, network security melalui segmentasi dan VLAN, host security dengan antivirus dan host-based firewall, application security dengan input validation dan authentication, serta data security melalui encryption dan access control. Pendekatan berlapis ini memastikan bahwa kegagalan satu layer security tidak akan mengkompromikan seluruh sistem keamanan. Logging adalah proses pencatatan event dan aktivitas jaringan yang sangat penting untuk security monitoring dalam mendeteksi aktivitas mencurigakan, troubleshooting untuk identifikasi dan resolusi masalah, compliance untuk memenuhi requirement audit dan regulasi, serta forensic analysis untuk investigasi incident keamanan. System logs seperti /var/log/syslog untuk system messages, /var/log/auth.log untuk authentication attempts, dan /var/log/kern.log untuk kernel messages memberikan informasi vital tentang aktivitas sistem yang dapat dianalisis untuk keperluan keamanan dan troubleshooting. Network monitoring tools seperti tcpdump sebagai command-line packet analyzer, Wireshark sebagai GUI-based network protocol analyzer, netstat untuk network connections dan routing table, serta ss sebagai socket statistics utility memberikan kemampuan untuk memantau dan menganalisis lalu lintas jaringan secara real-time. Tools ini sangat penting dalam implementasi dan maintenance sistem keamanan jaringan yang efektif. Pemahaman komprehensif terhadap konsep-konsep dasar ini sangat penting untuk membangun infrastruktur jaringan yang aman, reliable, dan scalable. Melalui pembelajaran hands-on dalam modul praktikum ini, mahasiswa akan mendapatkan pengalaman praktis yang valuable untuk mengembangkan karir di bidang jaringan komputer dan cybersecurity, sekaligus mempersiapkan diri untuk menghadapi tantangan keamanan jaringan yang terus berkembang di era digital.

2 Tugas Pendahuluan

1. Diberikan studi kasus untuk konfigurasi VPN IPSec. Suatu erusahaan ingin membuat koneksi aman antara kantor pusat dan cabang. Jelaskan secara detail:

   (a) Fase negosiasi IPSec (IKE Phase 1 dan Phase 2)

   IKE Phase 1 (Main Mode)
   IKE Phase 1 bertujuan untuk membangun SA (Security Association) yang aman antara dua peer untuk melindungi komunikasi IKE selanjutnya.

   Langkah-langkah IKE Phase 1:

   i. Policy Negotiation: Kedua peer bertukar proposal keamanan termasuk algoritma enkripsi, hash, metode autentikasi, dan Diffie-Hellman group
   ii. Diffie-Hellman Key Exchange: Pertukaran kunci publik untuk menghasilkan shared secret
   iii. Authentication: Verifikasi identitas menggunakan pre-shared key, digital certificate, atau RSA signature
   iv. IKE SA Establishment: Pembentukan IKE Security Association yang aman

   IKE Phase 2 (Quick Mode)
   IKE Phase 2 menggunakan IKE SA yang telah dibentuk untuk menegosiasikan IPSec SA

yang akan melindungi data user.

Langkah-langkah IKE Phase 2:

i. IPSec Policy Negotiation: Negosiasi parameter IPSec seperti protokol (ESP/AH), algoritma enkripsi dan autentikasi
ii. Key Generation: Menghasilkan kunci enkripsi dan autentikasi untuk IPSec
iii. IPSec SA Creation: Pembentukan IPSec Security Association bidirectional
iv. Data Transfer: Mulai enkripsi dan transfer data menggunakan IPSec

(b) Parameter keamanan yang harus disepakati (algoritma enkripsi, metode autentikasi, lifetime key)

IKE Phase 1 Parameters:

- Algoritma Enkripsi: AES-256, 3DES, atau DES
- Hash Algorithm: SHA-256, SHA-1, atau MD5
- Metode Autentikasi: Pre-shared key, RSA signature, atau digital certificate
- Diffie-Hellman Group: Group 14 (2048-bit), Group 5 (1536-bit), atau Group 2 (1024-bit)
- Lifetime: 28800 detik (8 jam) sebagai default

IKE Phase 2 Parameters:

- Protokol Keamanan: ESP (Encapsulating Security Payload) atau AH (Authentication Header)
- Algoritma Enkripsi: AES-256, AES-128, 3DES
- Algoritma Autentikasi: SHA-256-HMAC, SHA-1-HMAC, MD5-HMAC
- PFS (Perfect Forward Secrecy): Ya/Tidak dengan DH group
- Lifetime: 3600 detik (1 jam) atau berdasarkan volume data

(c) Konfigurasi sederhana pada sisi router untuk memulai koneksi IPSec site-to-site

Konfigurasi Router Kantor Pusat (Cisco):

```
! IKE Phase 1 Policy
crypto isakmp policy 10
 encr aes 256
 hash sha256
 authentication pre-share
 group 14
 lifetime 28800

! Pre-shared Key
crypto isakmp key cisco123 address 203.0.113.2

! IKE Phase 2 Transform Set
crypto ipsec transform-set MYSET esp-aes 256 esp-sha256-hmac

```

```
! Crypto Map
crypto map VPNMAP 10 ipsec-isakmp
 set peer 203.0.113.2
 set transform-set MYSET
 match address VPN_TRAFFIC
 set pfs group14

! Access List untuk VPN Traffic
ip access-list extended VPN_TRAFFIC
 permit ip 192.168.1.0 0.0.0.255 192.168.2.0 0.0.0.255

! Apply ke Interface
interface GigabitEthernet0/1
 crypto map VPNMAP

```

Konfigurasi Router Kantor Cabang (Cisco):

```
! IKE Phase 1 Policy
crypto isakmp policy 10
 encr aes 256
 hash sha256
 authentication pre-share
 group 14
 lifetime 28800

! Pre-shared Key
crypto isakmp key cisco123 address 203.0.113.1

! IKE Phase 2 Transform Set
crypto ipsec transform-set MYSET esp-aes 256 esp-sha256-hmac

! Crypto Map
crypto map VPNMAP 10 ipsec-isakmp
 set peer 203.0.113.1
 set transform-set MYSET
 match address VPN_TRAFFIC
 set pfs group14

! Access List untuk VPN Traffic
ip access-list extended VPN_TRAFFIC
 permit ip 192.168.2.0 0.0.0.255 192.168.1.0 0.0.0.255

! Apply ke Interface
interface GigabitEthernet0/1
 crypto map VPNMAP

```

2. Sebuah sekolah memiliki bandwidth internet 100 Mbps yang dibagi menjadi:

   (a) 40 Mbps untuk e-learning

   (b) 30 Mbps untuk guru & staf (akses email, cloud storage)

   (c) 20 Mbps untuk siswa (browsing umum)

(d) 10 Mbps untuk CCTV & update sistem

Pembagian Bandwidth:

- E-learning: 40 Mbps (40
- Guru & Staf: 30 Mbps (30
- Siswa: 20 Mbps (20
- CCTV & Update Sistem: 10 Mbps (10

3. Buatlah skema Queue Tree yang lengkap:

(a) Parent dan child queue

```
TOTAL-DOWNLOAD (100Mbps)
├── E-LEARNING-DOWN (40Mbps) - Priority 1
├── GURU-STAF-DOWN (30Mbps) - Priority 2
├── SISWA-DOWN (20Mbps) - Priority 3
└── CCTV-SYSTEM-DOWN (10Mbps) - Priority 4

TOTAL-UPLOAD (100Mbps)
├── E-LEARNING-UP (40Mbps) - Priority 1
├── GURU-STAF-UP (30Mbps) - Priority 2
├── SISWA-UP (20Mbps) - Priority 3
└── CCTV-SYSTEM-UP (10Mbps) - Priority 4
```

(b) Penjelasan marking

Mangle Rules untuk Marking:

```
# Mark E-learning Traffic
/ip firewall mangle
add chain=prerouting src-address=192.168.10.0/24 action=mark-connection new-connection-mark=elearning-conn
add chain=prerouting connection-mark=elearning-conn action=mark-packet new-packet-mark=elearning-packet

# Mark Guru & Staf Traffic
add chain=prerouting src-address=192.168.20.0/24 action=mark-connection new-connection-mark=guru-staf-conn
add chain=prerouting connection-mark=guru-staf-conn action=mark-packet new-packet-mark=guru-staf-packet

# Mark Siswa Traffic
add chain=prerouting src-address=192.168.30.0/24 action=mark-connection new-connection-mark=siswa-conn
add chain=prerouting connection-mark=siswa-conn action=mark-packet new-packet-mark=siswa-packet

# Mark CCTV & System Traffic
add chain=prerouting src-address=192.168.40.0/24 action=mark-connection new-connection-mark=cctv-system-conn
add chain=prerouting connection-mark=cctv-system-conn action=mark-packet new-packet-mark=cctv-system-packet

```

(c) Prioritas dan limit rate pada masing-masing queue

Parent Queue:

```
# Parent Queue Download
/queue tree
add name=TOTAL-DOWNLOAD parent=ether1-gateway packet-mark="" limit-at=0 max-limit=100M priority=8

add name=TOTAL-UPLOAD parent=ether1-gateway packet-mark="" limit-at=0 max-limit=100M priority=8

```

Child Queue Download:

```
# E-learning Queue (Priority 1 - Highest)
/queue tree
add name=E-LEARNING-DOWN parent=TOTAL-DOWNLOAD packet-mark=elearning-packet limit-at=30M max-limit=40M priority=1 burst-limit=50M burst-threshold=35M burst-time=30s

# Guru & Staf Queue (Priority 2)
add name=GURU-STAF-DOWN parent=TOTAL-DOWNLOAD packet-mark=guru-staf-packet limit-at=20M max-limit=30M priority=2 burst-limit=40M burst-threshold=25M burst-time=20s

# Siswa Queue (Priority 3)
add name=SISWA-DOWN parent=TOTAL-DOWNLOAD packet-mark=siswa-packet limit-at=10M max-limit=20M priority=3 burst-limit=25M burst-threshold=15M burst-time=15s

# CCTV & System Queue (Priority 4)
add name=CCTV-SYSTEM-DOWN parent=TOTAL-DOWNLOAD packet-mark=cctv-system-packet limit-at=5M max-limit=10M priority=4

```

Child Queue Upload:

```
# E-learning Upload Queue
/queue tree
add name=E-LEARNING-UP parent=TOTAL-UPLOAD packet-mark=elearning-packet limit-at=30M max-limit=40M priority=1 burst-limit=50M burst-threshold=35M burst-time=30s

# Guru & Staf Upload Queue
add name=GURU-STAF-UP parent=TOTAL-UPLOAD packet-mark=guru-staf-packet limit-at=20M max-limit=30M priority=2 burst-limit=40M burst-threshold=25M burst-time=20s

# Siswa Upload Queue
add name=SISWA-UP parent=TOTAL-UPLOAD packet-mark=siswa-packet limit-at=10M max-limit=20M priority=3 burst-limit=25M burst-threshold=15M burst-time=15s

# CCTV & System Upload Queue
add name=CCTV-SYSTEM-UP parent=TOTAL-UPLOAD packet-mark=cctv-system-packet limit-at=5M max-limit=10M priority=4
```

```
13
```

Penjelasan Parameter Queue:

- limit-at: Bandwidth minimum yang dijamin
- max-limit: Bandwidth maksimum yang bisa digunakan
- priority: Prioritas queue (1=highest, 8=lowest)
- burst-limit: Bandwidth tambahan saat ada kapasitas lebih
- burst-threshold: Batas untuk mengaktifkan burst
- burst-time: Durasi burst maksimum

Dari tiap jawaban yang kalian berikan wajib memberikan referensi

2.1 Referensi

1. Stallings, W. (2017). Cryptography and Network Security: Principles and Practice (7th ed.). Pearson Education.
2. Cisco Systems. (2023). Cisco IOS Security Configuration Guide: Securing IP Multicast. Retrieved from https://www.cisco.com/c/en/us/support/docs/security-vpn/ipsec-negotiation-ike-protocols/
3. MikroTik. (2024). RouterOS Manual - Queue Tree. MikroTik Documentation. Retrieved from https://help.mikrotik.com/docs/display/ROS/Queue+Tree
4. Kurose, J. F., & Ross, K. W. (2021). Computer Networking: A Top-Down Approach (8th ed.). Pearson.
5. Forouzan, B. A., & Mosharraf, F. (2020). Computer Networks: A Top-Down Approach (2nd ed.). McGraw-Hill Education.
6. RFC 2401. (1998). Security Architecture for the Internet Protocol. Internet Engineering Task Force.
7. RFC 2409. (1998). The Internet Key Exchange (IKE). Internet Engineering Task Force.
8. MikroTik Academy. (2023). Traffic Management and QoS Implementation Guide. Retrieved from https://academy.mikrotik.com/
9. Lammle, T. (2020). CCNA Routing and Switching Complete Study Guide (2nd ed.). Sybex.
10. Pepelnjak, I. (2019). Network Security Technologies and Solutions. Cisco Press.