International Journal of Research in Engineering and Modern Technology (IJREMTE)
Volume 2, No 1, April 2025, Pages 22-30
ISSN 3089-4077

Design of Firewall Implementation Based on Deep Packet Inspection to Enhance Corporate Network Security

Nonot Wisnu Karyanto[1], Tjatursari Widiartin[2]

[1]Study Program of Computer Science, Faculty of Engineering, Wijaya Kusuma University Surabaya.
nonotwk@uwks.ac.id
[2]Study Program of Computer Science, Faculty of Engineering, Wijaya Kusuma University Surabaya.
widiartin@gmail.com

*Correspondence: nonotwk@uwks.ac.id

Abstract— To improve the security of increasingly complex and rapidly evolving digital data, a company needs to build a strong and secure data network by conducting research into the developments in data and network security technology. In the field of network security, there is a design of firewalls based on Deep Packet Inspection that can help analyze data up to the application or protocol level with the goal of detecting more complex data attack threats. By developing this system security design, better and stronger data security can be achieved.

Keywords— improve the security; digital data; Deep Packet Inspection; detecting more complex data attack threats

I. Introduction

The rapid development of information and communication technology drives companies to increasingly rely on computer networks as the backbone of their operations and business services. However, the increase in the volume and complexity of data traffic also brings the risk of increasingly sophisticated cyber attacks, such as malware injection, Distributed Denial of Service (DDoS), and application-based attacks (HTTP flood, SQL injection). Traditional firewalls—which generally only filter based on ports, protocols, and IP addresses—often fail to detect advanced attacks that exploit application payloads or use 'legitimate' ports to infiltrate. From the above issues, a problem formulation can be made as follows:

1. What are the advantages and disadvantages of DPI-based firewalls compared to conventional firewalls?
2. How effective is DPI in detecting malicious traffic in real-time?
3. How significant is the impact of DPI on network performance?

The objectives of this research are as follows:
1. To design and build a firewall system using DPI technology.
2. To analyze the effectiveness of DPI compared to conventional firewalls (stateful/stateless).
3. To enhance the security of the internal network against content-based attacks such as malware, spam, and command-and-control traffic.

II. Literature Review

Computer networks are a collection of two or more computer devices that are connected to each other through communication media (wired or wireless) with the aim of sharing data, information, hardware (such as printers), and other resources [1]. Operating System (OS) is the core software that manages all computer resources, including hardware and software, and acts as a bridge between the user and the computer hardware [4]. Computer attacks are efforts made by individuals or groups to access, damage, steal, disrupt, or interfere with computer systems, networks, or data, either illegally or without permission [8]

A firewall is a network security system that functions to control and filter data traffic that enters and exits a network or device, based on established security rules. A firewall can be in the form of hardware, software, or a combination of both. [10]

Deep Packet Inspection (DPI) is a network data analysis technique that allows network devices (such as firewalls, routers, or security systems) to thoroughly examine the contents of data packets passing through the network, not just the header but also the payload (content) of the packet.[12]

III. MATERIALS AND METHODS

In this study, the following steps will be undertaken:

1. System Design: architecture diagram for the DPI firewall.
2. System Implementation: installation and configuration of the DPI engine.
3. System Testing: simulation of attacks (DoS, XSS, malware download).
4. Effectiveness Evaluation: using metrics such as throughput, latency, detection rate, false positive/negative rate.

3.1. System Design Before conducting a more in-depth study in this research, it is necessary to first design the work steps in a diagram so that the results obtained align with the main objectives of this research. Below is the architecture design diagram of the DPI firewall:

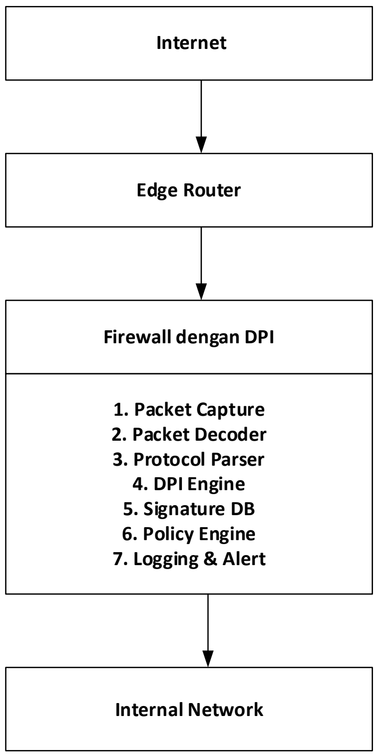

Figure 1. DPI firewall architecture diagram.

Explanation :

1. Internet

The Internet is a network of various networks that uses a standard communication protocol called TCP/IP to connect devices such as computers, smartphones, servers, routers, and others.

2. Edge Router

An Edge Router is a network device that is located at the boundary (edge) between the internal (private) network and the external network (usually the Internet). Its function is to connect and manage the data traffic entering and exiting the local network to the outside world.

3. Firewall with DPIA firewall with DPI is a network security device that filters traffic based on the content of the data comprehensively, not just based on basic rules such as IP addresses and ports. DPI allows the firewall to detect and prevent Layer 7 (Application Layer) attacks such as malware, exploits, and data leaks.

Explanation of the main components of a Firewall :

- Packet Capture
  Capturing all traffic that passes through the firewall, including header and payload data.
- Packet Decoder
  Analyzing the structure of packets (TCP, UDP, ICMP, etc.) to be forwarded to the next process.
- Protocol Parser
  Understanding application protocols such as HTTP, FTP, DNS, SSL to examine deeper content
- DPI Engine
  Analyzing packet payloads using deep inspection techniques, such as pattern matching or heuristic analysis.
- Signature Database
  Contains recognized patterns from threats such as malware, DDoS attacks, command-and-control traffic, etc.
- Policy Engine
  Determines actions based on DPI results and security policies (for example: drop, allow, quarantine, log).
- Logging & Alerting
  Records significant events and provides alerts to the SIEM (Security Information and Event Management) system or administrator.
- Internal Network
  Internal network is a part of the computer network that has restricted access only for users, devices, or systems within an organization or company. This network is not directly connected to the internet and is usually protected by firewalls, proxies, or other security systems.

3.2. System Implementation: Installation and Configuration of the DPI Engine

System Preparation :

- OS: Linux (Ubuntu/Debian/CentOS) is highly recommended
- Tools: git, gcc, make, libpcap-dev, python3, cmake

a. *Clone Repository* nDPI

```
git clone https://github.com/ntop/nDPI.git
cd nDPI
```

Figure 2. Coding Clone Repository

b. Build & Compile

```
mkdir build
cd build
cmake ..
make
sudo make install
```

Figure 3. Coding Build & Compile Section

.c. DPI Engine

Test Example of running the nDPI demo for pcap file inspection:

```
./example/ndpiReader -i ../tests/pcap/Skype-facebook.pcap
```

Figure 4. Coding snippet of the DPI Engine test

DPI Configuration (General)

- Filter specific protocols: HTTP, HTTPS, DNS, SSH, FTP, etc.
- Custom rules: payload detection (such as signatures for malware)

• Integration with firewall (e.g.: iptables or nftables)

Integration with Network SystemsThe DPI engine can be integrated with:

• Firewall: as an intelligent filtering module
• IDS/IPS: for real-time attack detection and prevention
• Proxy Server: for HTTP/S inspection
• NetFlow/sFlow collector: for traffic analysis

3.3. System Testing: attack simulation (DoS, XSS, malware download).

Here is a complete explanation for testing network security systems through attack simulations such as DoS (Denial of Service), XSS (Cross-site Scripting), and malware downloads, particularly in the context of testing the effectiveness of DPI (Deep Packet Inspection) systems, firewalls, or IDS/IPS.

System Testing: Attack Simulation (DoS, XSS, Malware Download)

Objectives of Testing :

• To test the effectiveness of the DPI Engine in detecting, blocking, or logging attacks
• To assess the security system's response to common types of attacks
• To ensure the system can filter or control malicious traffic.

DoS Attack Simulation (Denial of Service)

Tools Used:

• hping3
• LOIC (Low Orbit Ion Cannon) or HOIC
• slowloris
• metasploit auxiliary/dos modules

Example: SYN Flood attack with hping3

```
sudo hping3 -S --flood -V -p 80 192.168.1.10
```

Figure 5. Coding snippet of SYN Flood attack

Explanation: Sending a large number of TCP SYN packets to port 80 (HTTP) of the target server

XSS (Cross-Site Scripting) Attack Simulation

Tools Used:

• Browser + Burp Suite / OWASP ZAP
• Payload Generator (XSSer, XSS Payloads repo)

XSS Payload Example:

```
<script>alert('XSS')</script>
```

Testing Method:

1. Send payload to the input parameter (form, URL, query string)
2. Monitor the reaction of DPI/IPS—whether the payload is flagged/dropped

Objective:

• To assess whether the system can detect/block harmful input in HTTP traffic.

3.4. Malware Download SimulationSafe

Tools and Sources:

• EICAR Test File (simulated virus file, not an actual harmful file)
• GTFOBins + Metasploit for exploiting harmful files
• Run an HTTP server then wget/curl the file from the target client:
curl http://yourserver.com/eicar.com -O

Things Tested:

Can the DPI/firewall:

1. Block downloads
2. Log activities
3. Give warnings

3.5 Monitoring and Logging

Use the following systems to monitor results:

1. nDPI + ntopng (DPI-based interface monitoring)
2. Suricata + Kibana for IDS with a visual log view
3. Grafana + Prometheus/InfluxDB for traffic and time-based alerts
4. SIEM tools such as Wazuh or Splunk (if installed)

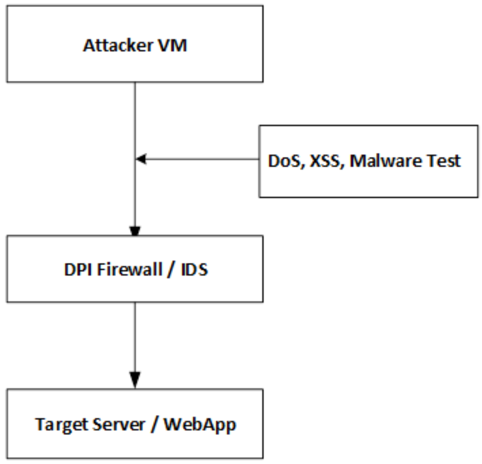

Figure 6. Test Architecture.

IV. Result and Discussion

4. 1. Effectiveness Evaluation: using metrics such as throughput, latency, detection rate, false positive/negative rate.

The following is an explanation for Effectiveness Evaluation in the context of network security systems (such as firewalls with Deep Packet Inspection - DPI), using metrics:

System Effectiveness Evaluation The effectiveness evaluation of the system is conducted to measure the performance and accuracy of the system in real conditions.

The metrics used include:

1. Throughput
   - Definition: The amount of data that is successfully processed by the system in a unit of time (e.g., Mbps or Gbps).
   - Purpose: To assess how well the system can handle network traffic without bottlenecks.
   - Evaluation Example: If DPI significantly slows down throughput, it needs to be optimized.

2. .Latency (Latency)
   - Definition: The delay that occurs between when data is sent and received (usually measured in milliseconds).
   - Purpose: To measure the impact of the system on the network response speed.
   - Evaluation Example: High latency on DPI can disrupt real-time services such as VoIP.

3. Detection Rate
   - Definition: The percentage of attacks or anomalies successfully detected by the system.
   - Purpose: To assess the accuracy of the system in detecting threats.

Formula :

$$Detection\ Rate = \left(\frac{True\ Positives}{True\ Positives + False\ Negatives}\right) x\ 100\% \quad (1)$$

4. False Positive Rate (FPR)
- Definition: The percentage of normal occurrences that are incorrectly classified as threats.
- Purpose: To assess the reliability of the system in avoiding false alarms.

Formula :

$$FPR = \left(\frac{False\ Positives}{False\ Positives + True\ Negatives}\right) x\ 100\% \quad (2)$$

5. False Negative Rate (FNR)
- Definition: The percentage of threats that are not detected by the system.
- Objective: To assess the security risks that are not addressed by the system.

Formula:

$$FNR = \left(\frac{False\ Negatives}{False\ Negatives + True\ Positives}\right) x\ 100\% \quad (3)$$

4.2. Data Simulation Results of DPI Firewall Testing:

Table 1. DPI Testing Simulation Values

No.	Category	Amount
1	True Positive (TP)	180
2	False Positive (FP)	20
3	True Negative (TN)	750
4	False Negative (FN)	50

1. Detection Rate

Formula :

$$Detection\ Rate = \left(\frac{TP}{TP + FN}\right) X\ 100\%$$

Calculation:

$$Detection\ Rate = (\frac{180}{180+50}) \text{x } 100\ \% = (\frac{180}{230}) \text{ x } 100\% \approx 78{,}26\%$$

2. False Positive Rate (FPR)

Formula :

$$FPR = (\frac{FP}{FP+TN})\ x\ 100\%$$

Calculation :

$$\text{FPR} = \left(\frac{20}{20+750}\right) x\ 100\% = \left(\frac{20}{770}\right) \text{x } 100\% \approx 2{,}60\%$$

3. False Negative Rate (FNR)
   Formula :

$$\text{FNR} = \left(\frac{\text{FN}}{FN+TP}\right) x\ 100\ \%$$

Calculation :

$$\text{FNR} = \left(\frac{50}{50+180}\right) x\ 100\% = \left(\frac{50}{230}\right) x\ 100\% \approx 21,\ 74\%$$

Example of Throughput & Latency
For instance, the performance test results of DPI:

- Throughput: 850 Mbps from a maximum capacity of 1 Gbps → 85% utilization
- Latency: 45 ms (before DPI 20 ms) → additional delay of 25 ms

Table 2. Testing Methods

No	Method	Results
1	*Detection Rate*	78,26%
2	*False Positive Rate* (FPR)	2,60%
3	False Negative Rate (FNR)	21,74%

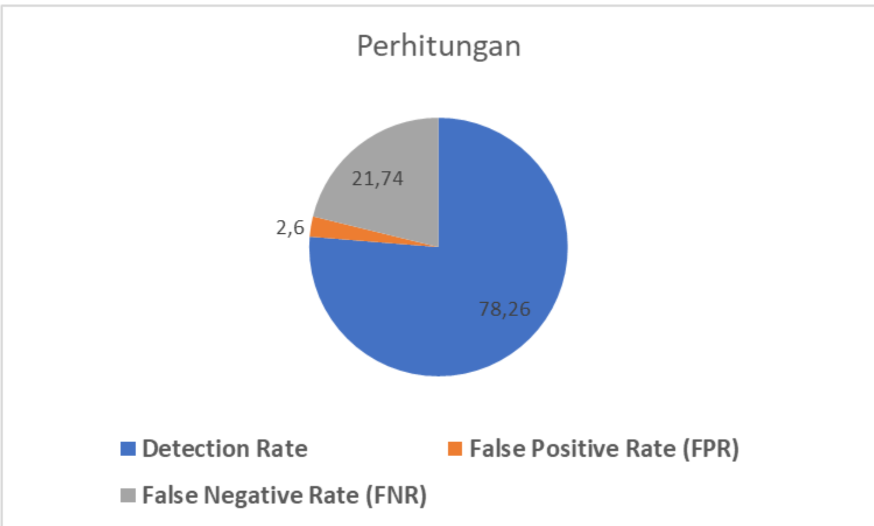

Figure 7 Graph of Test Results

4.3. Evaluate the simulation

1. The system detects threats well (Detection Rate ~78.26%).
2. The number of false alarms is very low (FPR ~2.60%).
3. However, there are still threats that passed through (FNR ~21.74%) — this can be improved with an update to the Signature DB.
4. The decline in network performance is still within reasonable limits (High Throughput, Latency is still tolerable).

V. Conclusion

Based on the results of the design and implementation of a firewall system based on Deep Packet Inspection (DPI) it can be concluded :

1. That this method is capable of significantly improving the security of the company's network. DPI allows for inspection of data traffic up to the application layer, making it more effective in detecting and blocking threats such as malware, DoS attacks, and suspicious traffic compared to traditional firewalls.

2. Implementation of this system also shows positive results in terms of threat detection rates and reduction of false positives, while maintaining stable network performance. Testing through attack simulations proves that the DPI firewall can provide quick and accurate responses in handling malicious traffic.

3. Therefore, the use of DPI-based firewalls becomes a relevant and efficient solution to strengthen the security of corporate network infrastructure, and can be further developed with the integration of other technologies such as SIEM systems and machine learning for more adaptive threat detection.

References

[1] Ata Elahi & Alex Cushman, Computer Networks: Data Communications, Internet and Security, edisi 2024.
[2] Mohamed Ali Zormati, Hicham Lakhlef, Sofiane Ouni, *Review and Analysis of Recent Advances in Intelligent Network Softwarization for the Internet of Things* Journal reference:Computer Networks, Volume 241, 2024, 110215, ISSN 1389-1286, Related DOI: https://doi.org/10.1016/j.comnet.2024.110215
[3] Wilson Cook, Best Computer Networking Books of 2025, Jan 13, 2025
[4] Abraham Silberschatz, Greg Gagne, dan Peter B. Galvin. *Operating System Concepts* (10th ed.) edisi 2021-2025.
[5] Andrew S. Tanenbaum dan Herbert Bos. *Modern Operating Systems* (5th ed., 2022–2024)
[6] Andrew S. Tanenbaum dan Albert Woodhull. *Operating Systems: Design and Implementation*, September 18, 2024
[7] Remzi dan Andrea Arpaci-Dusseau, *Operating Systems: Three Easy Pieces* (OSTEP), Februari 12, 2025.
[8] Check Point Software's 2025 Security Report Finds Alarming 44% Increase in Cyber-Attacks Amid Maturing Cyber Threat Ecosystem, Redwood City, CA — Tue, 14 Jan 2025
[9] Q1 2025 Global Cyber Attack Report from Check Point Software: An Almost 50% Surge in Cyber Threats Worldwide, with a Rise of 126% in Ransomware Attacks
[10] Dublin, Feb. 24, 2025 (GLOBE NEWSWIRE) -- *The "Firewall-as-a-Service Market Report 2025*" report has been added to ResearchAndMarkets.com's offering.

[11] Qi Duan, Ehab Al-Shaer, Firewall Regulatory Networks for Autonomous Cyber Defense, 24 April 2025.
[12] Deep Packet Inspection Market Trends 2025: AI-Powered DPI, Cybersecurity Innovations, and Market Growth Insights,https://www.openpr.com/news/3951980/deep-packet-inspection-market-trends-2025-ai-powered-dpi
[13] Danaswara Prawira Harja, Andrian Rakhmatsyah, Muhammad Arief Nugroho, Implementasi Metode Deep Packet Inspection untuk Meningkatkan Keamanan Jaringan pada Software Defined Networks, Ind. Journal on Computing Vol. 4, Issue. 1, March 2019. pp. 133-146 doi:10.21108/indojc.2019.4.1.286.
[14] https://www.imarcgroup.com/next-gene
[15] Rianda Pratama Literature Review : *Network Security Menggunakan Virtual Private Network L2TP/IPSEC, Port Knocking, Port Forwarding, Honeypot Dan Pfsense*, Jurnal Jaringan Komputer dan Keamanan JJKK, Vol. 04, No. 03, October 2023: 11-1
[16] Dwi Bayu Rendro, Ngatono,Wahyu Nugroho Aji : *ANALISIS MONITORING SISTEM KEAMANAN JARINGAN KOMPUTER MENGGUNAKAN SOFTWARE NMAP (STUDI KASUS DI SMK NEGERI 1 KOTA SERANG)* Jurnal PROSISKO Vol. 7 No. 2 September 2020 ISSN : 2406-7733 e-ISSN :2597-9922.

[17] Sugi Aprianti1, Riska, Hendri Alamsyah : *Analisa Keamananaan Jaringan Komputer Menggunakan Sistem Deteksi Intrusi Shorewall*, Jurnal Amplifier Mei 2023 Vol 13 No 1 P-ISSN 2089-2020 dan E-ISSN 2622-2000

[18] CL Ari Setiawan, Zulfikri, Adhamdi Tria Putra Abza, *: Sistem Keamanan Jaringan Komputer Metode Network Intrusion Detection System Di Kantor Setwan*, Jurnal Intra-Tech Vol 4 No 2 (2020)

[19] Nopri Dwipoyono, Khairil, Aji Sudarsono : *Penerapan Firewall Pada Sistem Keamanan Jaringan Komputer Di Sekolah SMK Negeri 5 Seluma*, Jurnal Media Infotama Vol. 19 No.2 2023 454

[20] Muhamad Fahrizal Rizqi, Rohmat Tulloh, Nazel Djibran:*Implementasi Web Application Firewall untuk Melindungi Aplikasi Web dari Serangan Malware,* Jurnal Informatika Universitas Pamulang, Vol. 8, No. 2, Juni 2023 (341-348).

[21] Sipho Nkosi, Thandeka Mthembu : *Firewall Mastery: Advanced Strategies for Implementation and Digital Defense*, International Journal of Trend in Scientific Research and Development (IJTSRD) Volume 4 Issue 3, April 2020 Available Online: www.ijtsrd.com e-ISSN: 2456 – 6470.

[22] Herika Andini Putri, Rohmat Tulloh, Nazel Djibran : *Implementasi Perangkat Next Generation Firewall untuk Melindungi Aplikasi dari Serangan Malware*, Jurnal Informatika Universitas Pamulang ISSN: 2541-1004 e-ISSN: 2622-4615 Vol. 8, No. 2, Juni 2023 (322-329) 10.32493/informatika.v8i2.33656.

[23] Reza Setya Budi, Irwan Sembiring *: IMPLEMENTASI KEAMANAN JARINGAN KOMPUTER DENGAN IPTABLES SEBAGAI FIREWALL MENGGUNAKAN PORT KNOCKING METODE DINAMIS,* Jurnal Ilmiah dan Pembelajaran Informatika, Vol 10, No 1 (2025)