

## ABSTRAK

Pengklasifikasian trafik data pada *firewall* tidak cukup bila hanya menggunakan parameter seperti nomor *port*. Saat ini banyak aplikasi yang bisa digunakan tanpa harus memakai nomor *port* yang seharusnya aplikasi tersebut gunakan. Selain itu, pengaturan akses pada web aplikasi menggunakan *firewall* juga tidak bisa bila hanya digunakan tiga parameter yang disebutkan di awal.

Metode *deep packet inspection* dapat dipakai pada *firewall* sebagai metode pengklasifikasian untuk digunakan dalam pengaturan akses trafik data. L7-Filter dan nDPI merupakan *deep packet inspection library* yang dapat digabungkan dengan aplikasi *firewall*. Tingkat kualitas L7-Filter dan nDPI sebagai pengklasifikasian data pada *firewall* akan diukur pada tugas akhir ini.

Berdasarkan hasil pengujian pada tugas akhir ini, nDPI memiliki performansi yang lebih bagus daripada L7-Filter, dalam hal nilai sensitivitas dan nilai spesifisitas. Nilai sensitivitas *rule firewall* yang menggunakan nDPI lebih tinggi 2,1% bila digunakan untuk menghentikan akses dan lebih tinggi 2.31% bila digunakan untuk menerima akses layanan, dibandingkan nilai sensitivitas L7-Filter. Sementara nilai spesifisitas *rule firewall* dengan nDPI lebih tinggi 2.26% saat digunakan untuk menghentikan layanan, dan lebih tinggi 6.66% jika digunakan untuk menerima akses layanan. Meskipun demikian, *rule firewall* yang menggunakan L7-Filter memiliki waktu pengeksekusian rata-rata yang lebih cepat 0.0298 ms dibandingkan nDPI.

**Kata Kunci** : *pengklasifikasian paket data, firewall, deep packet inspection, L7-Filter, nDPI.*

## ABSTRACT

Traffic data classification for access management in firewall is insufficient when using parameter like port number. Nowadays, many applications can be properly executed without using its standard port. Web application blocking access using firewall, can't be done using ip address as the only classification parameter.

Deep packet inspection methods can be used in firewall as packet data classifier for traffic data access management. L7-Filter and nDPI are deep packet inspection library which can be combined with firewall, as packet data classifier. The classification quality of L7-Filter and nDPI as firewall will be tested in this thesis (final task).

According to L7-Filter and nDPI testing scenario result in this thesis, nDPI has better performance in firewall rule sensitivity and specificity. nDPI's sensitivity is better than L7-Filter's, 2.1% when used for blocking access and 2.31% when used for accepting access. nDPI's specificity is better than L7-Filter's, 2.26% when used for blocking access and 6.66% when used for accepting access. The L7-Filter firewall rule execution time, however, is faster 0.0298 ms than nDPI.

**Keyword:** *packet data classification, firewall, deep packet inspection, L7-Filter, nDPI*