UJI KINERJA DMZ (DE-MILITARIZED ZONE) DENGAN SIMULATOR GNS3 (GRAPHICAL NETWORK SIMULATOR)

Irma Wira Sari Putri[11], Lalu Syamsul Irfan A.[2], A. Sjamsjiar Rachman[3]

ABSTRAK

Salah satu solusi sistem keamanan dalam membangun sebuah jaringan adalah dengan menerapkan *firewall* DMZ yang merupakan suatu sistem jaringan keamanan yang terletak antara jaringan pribadi dan jaringan publik. DMZ (*Demilitarized Zone)* membuat segmentasi jaringan untuk meletakkan server yang bisa diakses publik dengan aman tanpa harus mengganggu sistem lain. Terdapat *iptables* dalam *firewall* yang digunakan untuk mengatur lalu lintas jaringan dengan menerapkan beberapa aturan yang dibuat untuk membatasi ataupun menolak suatu koneksi pada jaringan tersebut. Membangun sebuah jaringan dapat dilakukan menggunakan simulator GNS3 (*Graphical Network Simulator*), yaitu suatu *software* simulasi jaringan komputer berbasis GUI. Dalam penelitian ini, pengujian dilakukan dengan meletakkan layanan *Web Server* dan FTP (*File Transfer Protocol)* pada server DMZ yang dapat diakses oleh publik. Kemudian menganalisa kualitas jaringan menggunakan iperf, aplikasi yang dapat digunakan untuk menguji kinerja jaringan. Adapun hasil yang didapat dari pengujian *bandwidth* dengan Iperf memiliki nilai rata-rata *jitter* cukup kecil pada masing-masing jaringan. Namun masih dikategorikan memiliki kualitas jaringan yang baik. Pada jaringan dengan konsep DMZ nilai rata-rata *jitter* sebesar 0.106 ms. Sedangkan jaringan tanpa konsep DMZ, nilai rata-rata *jitter* 0.456 ms.

Kata Kunci : *Firewall,* DMZ, *Iptables,* GNS3, Iperf.

ABSTRACT

Wrong one solution system security in build a network is with apply the DMZ firewall which is something system network security is between network personal and network the public. DMZ (*Demilitarized Zone)* make segmentation network for put down a server that can accessed public with secure without should disturb another system. Is available *iptables* in *firewalls* that are used for set then crossing network with apply some rules made for limit or reject something connection on network that is. Build a network could do use the GNS3 (*Graphical Network Simulator)* simulator, that is something simulation *software* network computer GUI based. In research this, testing do with put service *Web Server* and FTP (*File Transfer Protocol)* on the DMZ server that can accessed by the public. Then analyze quality network use iperf, applications that can used for test the performance network. As for results obtained from testing *bandwidth* with iperf have the average *jitter* is enough small on each network. However still categorized as have quality a good network. On network with the DMZ concept is the average value of *jitter* amounting to 0.106 ms. While network without DMZ concept, the average value of *jitter* is 0.456 ms.

Keywords : *Firewall,* DMZ, *Iptables,* GNS3, Iperf.

[1] Jurusan Teknik Elektro Fakultas Teknik Universitas Mataram, Nusa Tenggara Barat, Indonesia
Email : *irma.wirasari@gmail.com, irfan@unram.ac.id, asrachman@unram.ac.id*

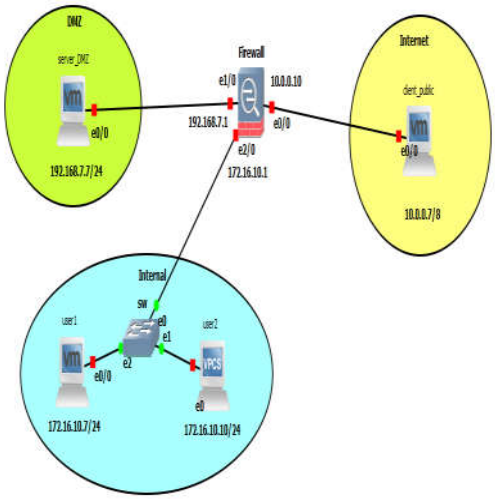
PENDAHULUAN

Firewall DMZ merupakan suatu sistem jaringan keamanan yang terletak dalam suatu jaringan LAN dan jaringan publik dengan membuat segmentasi jaringan untuk meletakkan server yang bisa diakses publik dengan aman tanpa harus bisa mengganggu keamanan sistem yang lain. *Firewall* diterapkan agar dapat melindungi jaringan dengan melakukan *filtrasi*, membatasi ataupun menolak suatu koneksi pada jaringan. Namun, untuk membangun sebuah jaringan diperlukan berbagai macam perangkat dan biaya yang cukup besar kerana mahalnya harga perangkat tersebut. Untuk itu, GNS3 yang merupakan simulator jaringan dapat dijadikan salah satu cara untuk menangani masalah diatas.

1. Perancangan Sistem

Perancangan sistem dibuat menggunakan simulator GNS3, dengan membangun dua buah topologi jaringan yang menggunakan konsep DMZ dan tanpa konsep DMZ.

a. Topologi dengan Konsep DMZ

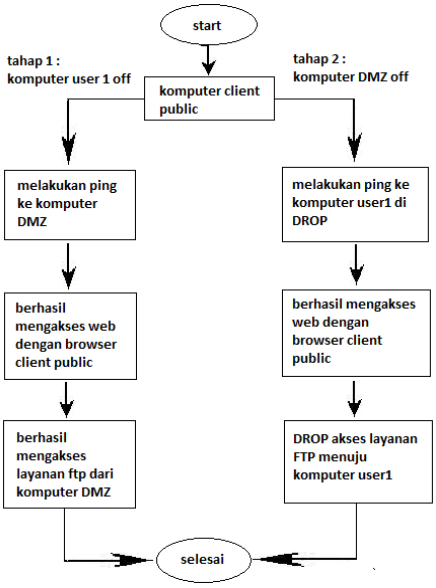


Gambar 1 Perancangan Topologi Jaringan dengan DMZ

Pada Gambar 1 diatas, merupakan perancangan topologi dengan menerapkan konsep DMZ dan menggunakan iptables sebagai firewall-nya yang akan diterapkan pada linux server. Beberapa aturan iptables diberikan untuk memberikan ataupun menolak akses layanan, yaitu web server dan FTP. Pengujian juga meliputi pengukuran kualitas jaringan menggunakan iperf.

1) Alur Pengujian

Pengujian dilakukan secara bertahap karena sistem perangkat yang digunakan penulis terbatas untuk bisa menjalankan semua perangkat virtual pada GNS3. Penulis mengalami masalah terkait dengan besarnya perangkat virtual yang harus dijalankan karena kemampuan RAM laptop penulis tidak mencukupi. Berikut gambar alur pengujian :



Gambar 2 Alur Pengujian

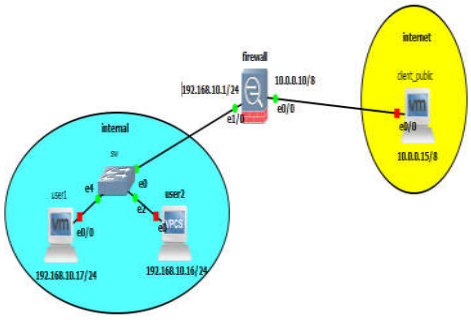
2) Aturan dalam Iptables

Adapun beberapa aturan iptables yang diterapkan pada firewall ditetapkan dalam file */etc/iptables.rules*. Berikut aturan iptables dalam gambar dibawah ini:

```
GNU nano 2.5.3                File: /etc/iptables.rules

# Generated by iptables-save v1.6.0 on Tue Oct 16 11:28:28 2018
*filter
:INPUT ACCEPT [72:5988]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [72:5988]
[0:0] -A FORWARD -s 10.0.0.7/32 -d 172.16.10.7/32 -p icmp -j DROP
[0:0] -A FORWARD -s 10.0.0.7/32 -d 172.16.10.7/32 -p tcp -m tcp --dport 80 -j ACCEPT
[0:0] -A FORWARD -s 10.0.0.7/32 -d 172.16.10.7/32 -p tcp -m tcp --dport 21 -j DROP
[0:0] -A FORWARD -s 10.0.0.7/32 -d 192.168.7.7/32 -p tcp -m tcp --dport 80 -j ACCEPT
[0:0] -A FORWARD -s 10.0.0.7/32 -d 192.168.7.7/32 -p tcp -m tcp --dport 21 -j ACCEPT
[0:0] -A FORWARD -s 192.168.7.7/32 -d 172.16.10.7/32 -p tcp -m tcp --dport 80 -j ACCEPT
[0:0] -A FORWARD -s 172.16.10.7/32 -d 192.168.7.7/32 -p tcp -m tcp --dport 80 -j ACCEPT
[0:0] -A FORWARD -s 172.16.10.7/32 -d 192.168.7.7/32 -p tcp -m tcp --dport 21 -j ACCEPT
[0:0] -A FORWARD -s 192.168.7.7/32 -d 172.16.10.7/32 -p tcp -m tcp --dport 21 -j ACCEPT
[0:0] -A FORWARD -p tcp -m tcp --dport 53 -j ACCEPT
[0:0] -A FORWARD -p udp -m udp --dport 53 -j ACCEPT
[0:0] -A FORWARD -p icmp -m icmp --icmp-type 8 -m length --length 86:65535 -j DROP
COMMIT
# Completed on Tue Oct 16 11:28:28 2018
# Generated by iptables-save v1.6.0 on Tue Oct 16 11:28:28 2018
*nat
:PREROUTING ACCEPT [0:0]
:INPUT ACCEPT [0:0]
:OUTPUT ACCEPT [463:29093]
:POSTROUTING ACCEPT [463:29093]
[0:0] -A POSTROUTING -s 192.168.7.0/24 -d 10.0.0.0/8 -j MASQUERADE
[0:0] -A POSTROUTING -s 172.16.10.0/24 -d 10.0.0.0/8 -j MASQUERADE
COMMIT
# Completed on Tue Oct 16 11:28:28 2018
```

Gambar 3 Aturan Iptables Topologi Jaringan dengan DMZ

b. Topologi tanpa Konsep DMZ



Gambar 4 Perancangan Topologi Jaringan tanpa DMZ

Perbedaan kedua gambar diatas adalah, Pada Gambar 2 layanan yang diberikan diletakkan dalam jaringan internal sehingga dapat dengan mudah di akses oleh pengguna internet. Sedangkan pada Gambar 1 layanan diletakkan dalam jaringan DMZ sengga tidak mengganggu jaringan internalnya.

1) Alur Pengujian
Alur pengujian pada topologi ini dijalankan secara keseluruhan. Karena sedikitnya perangkat virtual yang digunakan sehingga masih dapat berjalan dengan kapasitas RAM penulis.

2) Aturan Iptables
Adapun beberapa aturan iptables yang diterapkan pada firewall ditetapkan dalam file */etc/iptables.rules*. Berikut aturan iptables dalam gambar dibawah ini:

```
GNU nano 2.5.3                File: /etc/iptables.rules

# Generated by iptables-save v1.6.0 on Tue Oct 16 11:01:40 2018
*filter
:INPUT ACCEPT [321:24008]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [342:25616]
[0:0] -A FORWARD -s 10.0.0.15/32 -d 192.168.10.17/32 -p tcp -m tcp --dport 21 -j DROI
[0:0] -A FORWARD -s 10.0.0.15/32 -d 192.168.10.17/32 -p tcp -m tcp --dport 80 -j ACCI
[0:0] -A FORWARD -s 10.0.0.15/32 -d 192.168.10.16/32 -p icmp -j DROP
[0:0] -A FORWARD -p tcp -m tcp --dport 53 -j ACCEPT
[56:3360] -A FORWARD -p udp -m udp --dport 53 -j ACCEPT
[0:0] -A FORWARD -p icmp -m icmp --icmp-type 8 -m length --length 86:65535 -j DROP
COMMIT
# Completed on Tue Oct 16 11:01:40 2018
# Generated by iptables-save v1.6.0 on Tue Oct 16 11:01:40 2018
*nat
:PREROUTING ACCEPT [88:6949]
:INPUT ACCEPT [8:1933]
:OUTPUT ACCEPT [884:53072]
:POSTROUTING ACCEPT [884:53072]
[68:4080] -A POSTROUTING -o eth0 -j MASQUERADE
[0:0] -A POSTROUTING -s 192.168.10.0/24 -j MASQUERADE
COMMIT
# Completed on Tue Oct 16 11:01:40 2018
```

Gambar 5 Aturan Iptables Topologi Jaringan tanpa DMZ

2. Hasil dan Pembahasan

1) Pengujian Layanan

a. Topologi dengan Konsep DMZ

Pada topologi ini, sesuai dengan alur pengujian yang telah di jelaskan diatas maka pengujian yang dilakukan secara terpisah.

Adapun pengujian pertama antara client public dengan server DMZ sebagai berikut :

1) Mengakses Web server
Client public mencoba untuk mengakses layanan web server pada jaringan DMZ melalui browser internet. Berikut gambar halaman web yang diakses:

Gambar 6 Halaman Web Server Jaringan DMZ

Pada Gambar 6 client public diizinkan mengakses web server pada port 80 menuju komputer DMZ sesuai dengan aturan yang diberikan. Berikut hasil Tabel aturan iptables :

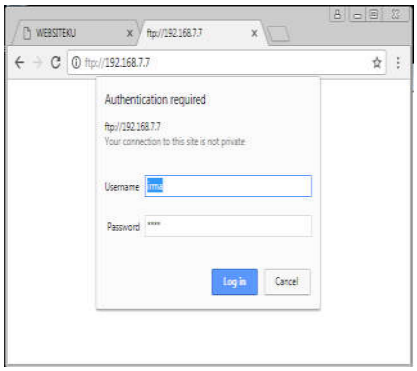
```
root@ubuntu:/home/server# iptables -L -n -v
Chain INPUT (policy ACCEPT 920 packets, 72590 bytes)
 pkts bytes target     prot opt in     out     source               destination

Chain FORWARD (policy ACCEPT 12 packets, 1155 bytes)
 pkts bytes target     prot opt in     out     source               destination
    0     0 DROP       icmp --  *      *       10.0.0.7             172.16.10.7
    0     0 ACCEPT     tcp  --  *      *       10.0.0.7             172.16.10.7          tcp dpt:80
    0     0 DROP       tcp  --  *      *       10.0.0.7             172.16.10.7          tcp dpt:21
    6   595 ACCEPT     tcp  --  *      *       10.0.0.7             192.168.7.7          tcp dpt:80
    0     0 ACCEPT     tcp  --  *      *       10.0.0.7             192.168.7.7          tcp dpt:21
    0     0 ACCEPT     tcp  --  *      *       192.168.7.7          172.16.10.7          tcp dpt:80
    0     0 ACCEPT     tcp  --  *      *       172.16.10.7          192.168.7.7          tcp dpt:80
    0     0 ACCEPT     tcp  --  *      *       172.16.10.7          192.168.7.7          tcp dpt:21
    0     0 ACCEPT     tcp  --  *      *       192.168.7.7          172.16.10.7          tcp dpt:21
    0     0 ACCEPT     tcp  --  *      *       0.0.0.0/0            0.0.0.0/0            tcp dpt:53
  102  6234 ACCEPT     udp  --  *      *       0.0.0.0/0            0.0.0.0/0            udp dpt:53
    0     0 DROP       icmp --  *      *       0.0.0.0/0            0.0.0.0/0            icmptype 8
length 86:65535

Chain OUTPUT (policy ACCEPT 972 packets, 74102 bytes)
 pkts bytes target     prot opt in     out     source               destination
```

Gambar 7 Tabel Iptables Web Server DMZ

Terlihat banyak paket yang dikirimkan sebesar 6 paket dengan ukuran 595 bytes.

2) Mengakses FTP

Client public mencoba untuk mengakses layanan FTP pada jaringan DMZ melalui internet. Berikut gambar halaman FTP pada browser :



Gambar 8 Halaman FTP

Pada Gambar 8 client public diizinkan mengakses FTP pada port 21 menuju komputer DMZ dengan melakukan login terlebih dahulu sesuai dengan aturan yang diberikan. Berikut hasil Tabel aturan iptables :

```
root@ubuntu:/home/server# iptables -L -n -v
Chain INPUT (policy ACCEPT 2399 packets, 186K bytes)
 pkts bytes target     prot opt in     out     source               destination

Chain FORWARD (policy ACCEPT 115 packets, 16126 bytes)
 pkts bytes target     prot opt in     out     source               destination
    0     0 DROP       icmp --  *      *       10.3.0.7             172.16.10.7
    0     0 ACCEPT     tcp  --  *      *       10.3.0.7             172.16.10.7         tcp dpt:80
    0     0 DROP       tcp  --  *      *       10.3.0.7             172.16.10.7         tcp dpt:21
    6   595 ACCEPT     tcp  --  *      *       10.3.0.7             192.168.7.7         tcp dpt:80
   66  3153 ACCEPT     tcp  --  *      *       10.3.0.7             192.168.7.7         tcp dpt:21
    0     0 ACCEPT     tcp  --  *      *       192.168.7.7          172.16.10.7         tcp dpt:80
    0     0 ACCEPT     tcp  --  *      *       172.16.10.7          192.168.7.7         tcp dpt:80
    0     0 ACCEPT     tcp  --  *      *       172.16.10.7          192.168.7.7         tcp dpt:21
    0     0 ACCEPT     tcp  --  *      *       192.168.7.7          172.16.10.7         tcp dpt:21
    0     0 ACCEPT     tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp dpt:53
  232 14282 ACCEPT     udp  --  *      *       0.0.0.0/0            0.0.0.0/0           udp dpt:53
    0     0 DROP       icmp --  *      *       0.0.0.0/0            0.0.0.0/0           icmptype 8
length 86:65535

Chain OUTPUT (policy ACCEPT 2544 packets, 192K bytes)
 pkts bytes target     prot opt in     out     source               destination
```

Gambar 9 Tabel Iptables FTP DMZ

Terlihat banyak paket yang dikirimkan sebesar 66 paket dengan ukuran 3153 bytes.

Pengujian kedua antara client public dengan user1 sebagai berikut :

1) Mengakses Web server

Client public mencoba untuk mengakses layanan web server pada jaringan internal komputer user1 melalui browser internet. Berikut gambar halaman web yang diakses:

Gambar 10 Halaman Web Server Jaringan Internal

Pada Gambar 10 client public diizinkan mengakses web server pada port 80 menuju komputer user1 sesuai dengan aturan yang diberikan. Berikut hasil Tabel aturan iptables :

```
root@ubuntu:/home/server# iptables -L -n -v
Chain INPUT (policy ACCEPT 17615 packets, 1363K bytes)
 pkts bytes target     prot opt in     out     source               destination

Chain FORWARD (policy ACCEPT 566 packets, 219K bytes)
 pkts bytes target     prot opt in     out     source               destination
    4   240 DROP       icmp --  *      *       10.0.0.7             172.16.10.7
   11  1289 ACCEPT     tcp  --  *      *       10.0.0.7             172.16.10.7         tcp dpt:80
    0     0 DROP       tcp  --  *      *       10.0.0.7             172.16.10.7         tcp dpt:21
    6   595 ACCEPT     tcp  --  *      *       10.0.0.7             192.168.7.7         tcp dpt:80
   66  3153 ACCEPT     tcp  --  *      *       10.0.0.7             192.168.7.7         tcp dpt:21
   10  1231 ACCEPT     tcp  --  *      *       192.168.7.7          172.16.10.7         tcp dpt:80
   22  1681 ACCEPT     tcp  --  *      *       172.16.10.7          192.168.7.7         tcp dpt:80
   52  3015 ACCEPT     tcp  --  *      *       172.16.10.7          192.168.7.7         tcp dpt:21
   56  3636 ACCEPT     tcp  --  *      *       192.168.7.7          172.16.10.7         tcp dpt:21
    0     0 ACCEPT     tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp dpt:53
 8188  542K ACCEPT     udp  --  *      *       0.0.0.0/0            0.0.0.0/0           udp dpt:53
    0     0 DROP       icmp --  *      *       0.0.0.0/0            0.0.0.0/0           icmptype 8
length 86:65535

Chain OUTPUT (policy ACCEPT 20892 packets, 1617K bytes)
 pkts bytes target     prot opt in     out     source               destination
```

Gambar 11 Tabel Iptables Web Server Internal

Terlihat banyak paket yang dikirimkan sebesar 11 paket dengan ukuran 1289 bytes.

2) Mengakses FTP

Client public mencoba untuk mengakses layanan FTP pada jaringan internal komputer user1 melalui internet. Berikut gambar halaman FTP pada browser :

Gambar 12 Halaman FTP

Pada Gambar 12 client public tidak diizinkan mengakses FTP pada port 21 menuju komputer user1. Sesuai dengan aturan yang telah diberikan bahwa FTP pada jaringan internal di blok. Berikut hasil Tabel aturan iptables :

```
root@ubuntu:/home/server# iptables -L -n -v
Chain INPUT (policy ACCEPT 17959 packets, 1389K bytes)
 pkts bytes target     prot opt in     out     source               destination

Chain FORWARD (policy ACCEPT 570 packets, 219K bytes)
 pkts bytes target     prot opt in     out     source               destination
    4   240 DROP       icmp --  *      *       10.0.0.7             172.16.10.7
   17  1553 ACCEPT     tcp  --  *      *       10.0.0.7             172.16.10.7          tcp dpt:80
    3   152 DROP       tcp  --  *      *       10.0.0.7             172.16.10.7          tcp dpt:21
    6   396 ACCEPT     tcp  --  *      *       10.0.0.7             192.168.7.7          tcp dpt:80
   66  3153 ACCEPT     tcp  --  *      *       10.0.0.7             192.168.7.7          tcp dpt:21
   10  1231 ACCEPT     tcp  --  *      *       192.168.7.7          172.16.10.7          tcp dpt:80
   22  1681 ACCEPT     tcp  --  *      *       172.16.10.7          192.168.7.7          tcp dpt:80
   52  3015 ACCEPT     tcp  --  *      *       172.16.10.7          192.168.7.7          tcp dpt:21
   56  3636 ACCEPT     tcp  --  *      *       192.168.7.7          172.16.10.7          tcp dpt:21
    0     0 ACCEPT     tcp  --  *      *       0.0.0.0/0            0.0.0.0/0            tcp dpt:53
 8331  552K ACCEPT     udp  --  *      *       0.0.0.0/0            0.0.0.0/0            udp dpt:53
    0     0 DROP       icmp --  *      *       0.0.0.0/0            0.0.0.0/0            icmptype 8
length 86:65535

Chain OUTPUT (policy ACCEPT 21264 packets, 1645K bytes)
 pkts bytes target     prot opt in     out     source               destination
```

Gambar 13 Tabel Iptables FTP DMZ

Terlihat banyak paket yang gagal dikirimkan sebesar 3 paket dengan ukuran 152 bytes.

b. Topologi tanpa Konsep DMZ

Sesuai dengan rancangan jaringan yang telah dibuat dalam topologi ini tidak menerapkan konsep DMZ, sehingga semua layanan yang diberikan diletakkan dalam jaringan internal.

1) Mengakses Web server

Client public mencoba untuk mengakses layanan web server pada jaringan internal komputer user1 melalui browser internet. Berikut gambar halaman web yang diakses:

Gambar 14 Halaman Web Server Jaringan Internal

Pada Gambar 14 client public diizinkan mengakses web server pada port 80 menuju komputer user1 sesuai dengan aturan yang diberikan. Berikut hasil Tabel aturan iptables :

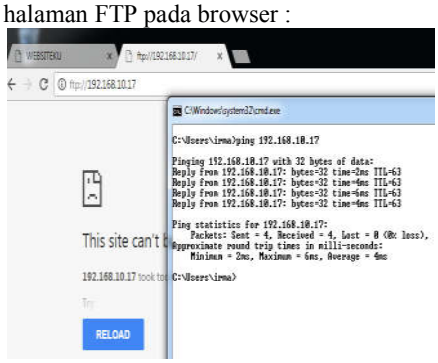
```
root@ubuntu:/home/server# iptables -L -v -n
Chain INPUT (policy ACCEPT 3978 packets, 304K bytes)
 pkts bytes target     prot opt in     out     source               destination

Chain FORWARD (policy ACCEPT 16 packets, 1827 bytes)
 pkts bytes target     prot opt in     out     source               destination
    0     0 DROP       tcp  --  *      *       10.0.0.15            192.168.10.17        tcp dpt:21
    8  1150 ACCEPT     tcp  --  *      *       10.0.0.15            192.168.10.17        tcp dpt:80
    0     0 DROP       icmp --  *      *       10.0.0.15            192.168.10.16
    0     0 ACCEPT     tcp  --  *      *       0.0.0.0/0            0.0.0.0/0            tcp dpt:53
  428 27024 ACCEPT     udp  --  *      *       0.0.0.0/0            0.0.0.0/0            udp dpt:53
    0     0 DROP       icmp --  *      *       0.0.0.0/0            0.0.0.0/0            icmptype 8
length 86:65535

Chain OUTPUT (policy ACCEPT 4292 packets, 325K bytes)
 pkts bytes target     prot opt in     out     source               destination
```

Gambar 15 Tabel Iptables Web Server Internal

Terlihat banyak paket yang dikirimkan sebesar 8 paket dengan ukuran 1150 bytes.

2) Mengakses FTP

Client public mencoba untuk mengakses layanan FTP pada jaringan internal komputer user1 melalui internet. Berikut gambar halaman FTP pada browser :



Gambar 16 Halaman FTP

Pada Gambar 16 client public tidak diizinkan mengakses FTP pada port 21 menuju komputer user1. Sesuai dengan aturan yang telah diberikan bahwa FTP pada jaringan internal di blok. Namun masih bias diakses dengan paket icmp/ping. Berikut hasil Tabel aturan iptables :

```
root@ubuntu:/home/server# iptables -L -v -n
Chain INPUT (policy ACCEPT 4826 packets, 367K bytes)
 pkts bytes target     prot opt in     out     source               destination

Chain FORWARD (policy ACCEPT 16 packets, 1827 bytes)
 pkts bytes target     prot opt in     out     source               destination
    3   152 DROP       tcp  --  *      *       10.0.0.15            192.168.10.17        tcp dpt:21
    8  1150 ACCEPT     tcp  --  *      *       10.0.0.15            192.168.10.17        tcp dpt:80
    0     0 DROP       icmp --  *      *       10.0.0.15            192.168.10.16
    0     0 ACCEPT     tcp  --  *      *       0.0.0.0/0            0.0.0.0/0            tcp dpt:53
  488 30624 ACCEPT     udp  --  *      *       0.0.0.0/0            0.0.0.0/0            udp dpt:53
    0     0 DROP       icmp --  *      *       0.0.0.0/0            0.0.0.0/0            icmptype 8
length 86:65535

Chain OUTPUT (policy ACCEPT 5160 packets, 390K bytes)
 pkts bytes target     prot opt in     out     source               destination
root@ubuntu:/home/server#
```

Gambar 17 Tabel Iptables FTP DMZ

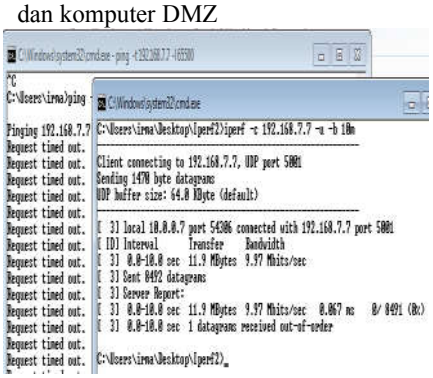
Terlihat banyak paket yang gagal dikirimkan sebesar 3 paket dengan ukuran 152 bytes.

2) Pengukuran Kualits Jaringan

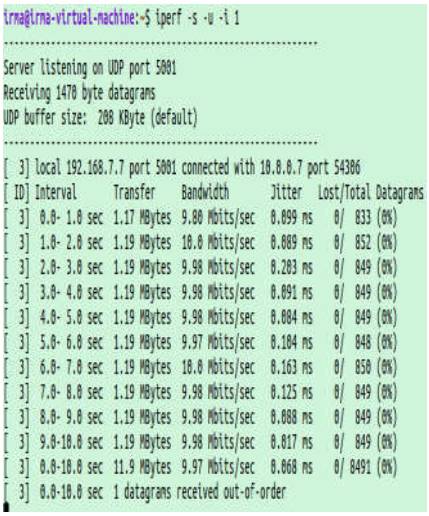
Pengukuran ini menggunakan tools monitoring iperf yang dijalankan pada dua sistem, yaitu pada sisi server dan sisi klien. Pengukuran dilakukan dengan mengganti nilai default bandwidth sebesar 10 Mbyte.

a. Topologi dengan Konsep DMZ

Pengujian antara komputer clien public dan komputer DMZ



Gambar 18 Pengukuran Bandwidth sisi Klien pada Server DMZ menggunakan Iperf.



Gambar 19 Pengukuran Bandwidth sisi Server pada Server DMZ menggunakan Iperf.

Disisi klien iperf server terkoneksi pada port server 5001, sedangkan disisi server iperf klien terkoneksi pada port 54386. Berikut rincian data yang diperoleh dapat dilihat dalam bentuk tabel :

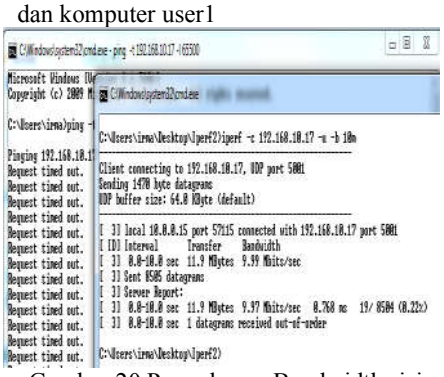
Tabel 1 Hasil Pengukuran Bandwidth pada Server DMZ dengan Iperf

Interval (s)	Transfer (Mbytes)	Bandwidth (Mbits/s)	Jitter (ms)
0-1	1.17	9.80	0.099
1-2	1.19	10.0	0.089
2-3	1.19	9.98	0.203
3-4	1.19	9.98	0.091
4-5	1.19	9.98	0.084
5-6	1.19	9.97	0.104
6-7	1.19	10.0	0.163
7-8	1.19	9.98	0.125
8-9	1.19	9.98	0.088
9-10	1.19	9.98	0.017

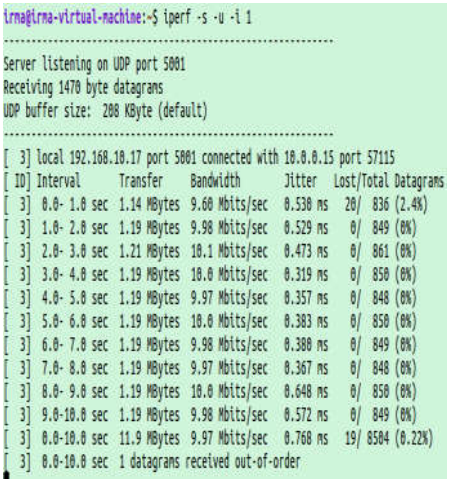
Dari tabel diatas diperoleh hasil dari nilai rata-rata jitter sebesar 0.106 ms, sehingga termasuk dalam kategori baik.

b. Topologi tanpa Konsep DMZ

Pengujian antara komputer clien public dan komputer user1



Gambar 20 Pengukuran Bandwidth sisi Klien pada komputer user1 menggunakan Iperf.



Gambar 21 Pengukuran Bandwidth sisi Server pada komputer user1 menggunakan Iperf.

Disisi klien iperf server terkoneksi pada port server 5001, sedangkan disisi server iperf klien terkoneksi pada port 57115.
Berikut rincian data yang diperoleh dapat dilihat dalam bentuk tabel :

Tabel 4.2 Hasil Pengukuran Bandwidth pada komputer user1 dengan Iperf

Interval (s)	Transfer (Mbytes)	Bandwidth (Mbits/s)	Jitter (ms)
0-1	1.14	9.60	0.530
1-2	1.19	9.98	0.529
2-3	1.21	10.1	0.473
3-4	1.19	10.0	0.319
4-5	1.19	9.97	0.357
5-6	1.19	10.0	0.383
6-7	1.19	9.98	0.380
7-8	1.19	9.97	0.367
8-9	1.19	10.0	0.648
9-10	1.19	9.98	0.572

Dari tabel diatas diperoleh hasil dari nilai rata-rata jitter sebesar 0.456 ms, sehingga termasuk dalam kategori baik.

Dari kedua pengukuran yang dilakukan pada masing-masing topologi didapati hasil yang cukup kecil, sehingga kualitas jaringan dikategorikan baik. Karena semakin kecil nilai jitter yang diperoleh, maka kualitas layanan jaringan yang dihasilkan semakin bagus, begitupun semakin besar nilai jitter maka semakin kurang bagus kualitas jaringan tersebut. Dari perbedaan antara kedua nilai rata-rata jitter diatas, maka dapat disimpulkan bahwa jaringan dengan konsep DMZ memiliki kualitas jaringan lebih baik dibandingkan dengan jaringan tanpa konsep DMZ. Ini karena nilai jitter yang dihasilkan lebih kecil.

3. Kesimpulan dan Saran

1. Kesimpulan

a. Simulator GNS3 membutuhkan RAM yang tinggi. Untuk standar RAM yang digunakan 2 GB dapat menjalankan beberapa perangkat router sedangkan untuk dapat menjalankan beberapa perangkat virtual mesin dibutuhkan RAM yang lebih besar dengan spesifikasi laptop atau komputer yang cukup tinggi.
b. Pada topologi dengan konsep DMZ, komputer *client public* berhasil mengakses layanan web dan ftp pada jaringan DMZ. Sedangkan pada jaringan internal, komputer *client public* hanya dapat mengakses layanan web sementara layanan ftp diblokir atau tidak dapat diakses.
c. DMZ berperan sebagai pengganti jaringan internal untuk beberapa layanan tertentu yang telah ditetapkan sebelumnya karena adanya pembagian zona. Dengan cara membatasi akses jaringan eksternal terhadap jaringan internal. Namun beberapa data yang ada dijaringan internal dapat diakses oleh komputer *client public* karena data tersebut diletakkan pada zona DMZ.
d. Pada topologi tanpa konsep DMZ, komputer *client public* berhasil melakukan akses layanan web pada jaringan internal. Sedangkan untuk layanan ftp pada jaringan internal diblok atau tidak dapat diakses sesuai dengan aturan yang diterapkan dalam *iptables.*

2. Saran

a. Simulator GNS3 memiliki spesifikasi yang tinggi, terutama dalam penggunaan RAM. Sehingga dianjurkan untuk menggunakan RAM yang memiliki kapasitas yang besar sesuai kebutuhannya.
b. Topologi yang dirancang memiliki keterbatasan akses layanan dan rules yang digunakan. Semakin banyak akses layanan yang diberikan maka kegunaan DMZ dalam jaringan dapat lebih optimal.
c. DMZ sangat bagus digunakan dalam keamanan sebuah jaringan karena dapat memberikan akses layanan berdasarkan zona yang diinginkan.

DAFTAR PUSTAKA

Aini, Qurrotul dan Victor Amrizal. (2010). *Implementasi IP-Tables Firewall pada Linux sebagai Sistem Keamanan Jaringan yang Handal. Jurnal Sistem Informasi, 3(1), 1-10.*

Basten, Marco Van. (2009). *Optimalisasi Firewall pada Jaringan Skala Luas*. Jurusan Teknik Informatika. Fakultas Ilmu Komputer. Universitas Sriwijaya.

Fauzie, Ahmad. (2004). *Analisis Penerapan Firewall sebagai Sistem Keamanan Jaringan pada PT. PLN (Persero) Penyaluran dan Pusat Pengatur Beban Jawa-Bali (P3B)*. Fakultas Sains dan Teknologi. Universitas Islam Negri Syarif Hidayatullah. Jakarta

Ikhwan, Syariful dan Ikhwana Elfitri. (2014). *Analisa Delay yang Terjadi Pada Penerapan De-militarized Zone (DMZ) terhadap Server Universitas Andalas. Jurnal Nasional Teknik Elektro, Vol.3, No.2, September 2014, 118-124.*

Juman, Kundang K. (2003). *Membangun Keamanan Jaringan Komputer Dengan sistem Demilitarized zone (DMZ). Jurnal Fasilkom, Vol.1, No.1, 1 Maret 2003, 12-29.*

Khasanah, Fata Nidaul. (2014). *Perancangan Dan Simulasi Jaringan Komputer Menggunakan Graphic Network Simulator 3 (GNS3)*. Program Studi Teknik Informatika. Fakultas Komunikasi Dan Informatika. Universitas Muhammadiyah Surakarta.

Kurniawan, Wiharsono. (2007). *Jaringan Komputer.* Yogyakarta: ANDI.

Mansfield, Niall. (2004). *Practical TCP/IP:Mendesain, Menggunakan, dan Troubleshooting Jaringan TCP/IP di Linux dan Windows (jilid 2)*. Yogyakarta: ANDI.

Pajri, Ria, Merry Agustina dan Qoriani Widayati. *Rancang Bangun Model Sistem Keamanan Jaringan Berbasis De-militarized Zone (DMZ) di Poltek Kementrian Kesehatan Palembang.* Universitas Bina Darma. Palembang.

Pribadi, H. (2004). *Router Linux menggunakan Freesco dan Floppy FW.* Yogyakarta: ANDI.

Rafiudin, R. (2006). *Membangun Firewall dan Traffic Filtering Berbasis CISCO*. (D. Hardjono, Ed.) (1st ed.). Yogyakarta: ANDI.

Setiawan, Agus. (2016). *Panduan Konfigurasi GNS3 untuk LAB Cisco-Nixtrain.* Bandung.

Sondakh, Glend, Meicsy E. I Najoan dan Arie S. Lumenta. (2014). *Perancangan Filtering Firewall Menggunakan Iptables Di Jaringan Pusat Teknologi Informasi Unsrat.* Jurusan Teknik Elektro. Fakultas Teknik. Universitas Sam Ratulangi. *E-journal Teknik Elektro dan Komputer (2014), ISSN : 2301-8402, 19-27.*

Sujito dan Mukhamad Fatkhur Roji. (2010). *Sistem Keamanan Internet Dengan Menggunakan IP Tables Sebagai Firewall. Jurnal ilmiah DINAMIKA DOTCOM Vol.1, No.1, 1 Januari 2010, 58-70.*

Sukmaaji, Anjik dan Rianto. (2008). *Jaringan Komputer: Konsep Dasar Pengembangan Jaringan dan Keamanan Jaringan.* Yogyakarta: ANDI.

Twelefty, Yuni, Tafta Zani, dan Muhammad Fahru Rizal. (2015). *Implementasi GNS3 Cluster sebagai Alat Bantu Simulasi Jaringan Komputer (Studi Kasus : Laboratorium Jaringan Komputer Fakultas Ilmu Terapan)*. Program Studi D3 Teknik Komputer. Fakultas Ilmu Terapan. Universitas Telkom. *E-proceeding of Applied Science : Vol.1, No.3, Desember 2015, ISSN : 2442-5826, 2377-2382*

Wahana Komputer. (2003). *Panduan Lengkap Pengembangan Jaringan Linux.* (1st ed.). Yogyakarta: ANDI.

IRMA WIRA SARI PUTRI
Lahir di Batuyang, Pringgabaya pada tanggal 10 Juli 1994. Menempuh Pendidikan Program Strata 1 (S1) di Fakultas Teknik Universitas Mataram sejak tahun 2012.