Matrik: Jurnal Manajemen, Teknik Informatika, dan Rekayasa Komputer
Vol. 20, No. 2, Mei 2021, pp. 283~292
ISSN: 2476-9843, accredited by Kemenristekdikti, Decree No: 200/M/KPT/2020
DOI: 10.30812/matrik.v20i1.1068

Analisis Performa *Access Control List* menggunakan Metode *Firewall Policy Base*

Performance Analysis of the Access Control List Using the Firewall Policy-Based Method

Firmansyah[1], Mochamad Wahyudi[2]
[1]Sekolah Tinggi Manajemen Informatika dan Komputer Nusa Mandiri, Indonesia
[2]Universitas Bina Sarana Informatika, Indonesia

Article Info

Article history:

Received, 7 Februari 2021
Revised, 17 April 2021
Accepted, 10 Mei 2021

Kata Kunci:

Jaringan Komputer
Cybercrime
Zone Based Policy Firewall
Access Control List

ABSTRAK

Pemanfaatan teknologi informasi mampu mendukung mobilitas yang begitu cepat dan sangat efesien. Kini, hampir semua transfer data dilakukan menggunakan jaringan komputer dan bersifat terbuka. dengan terjadinya transfer data yang bersifat terbuka hal ini mampu memicu terjadinya kejahatan didalam dunia jaringan komputer (*cybercrime*). Penerapan keamanan jaringan komputer merupakan hal yang sangat vital. untuk memiminalisir *cybercrime* didalam jaringan komputer, maka diterapkanlah keamanan jaringan menggunakan metode *zone-based policy firewall. Zone-based policy firewall* mampu melakukan pembatasan akses berdasarkan mekanisme keamanan yang digunakan untuk melindungi sistem internal dari gangguan para pelaku *Cybercrime* atau pihak-pihak lain yang ingin memasuki kedalam sistem tanpa mempunyai hak akses. dari hasil penelitian analisa performa *access control list* menggunakan metode *zon based policy firewall* didapatkan penerapan keamanan jaringan komputer *zone-based policy firewall* mampu membatasi akses menuju *server* dari *client* yang terhubung didalam jaringan yang sama. Serta *zone-based policy firewall* mampu menyembunyikan *hop count* yang dilalui untuk menghubungkan antara *client* dengan *server*.

Keywords:

Computer Network
Cybercrime
Zone Based Policy Firewall
Access Control List

ABSTRACT

The use of information technology is able to support mobility that is so fast and very efficient. Today, almost all data transfers are done using computer networks and are open in nature. With the occurrence of open data transfer, it is able to trigger crime in the world of computer networks (cybercrime). The application of computer network security is very vital. To minimize cybercrime in computer networks, network security is implemented using a zone-based policy firewall method. Zone-based policy firewalls are able to restrict access based on security mechanisms used to protect internal systems from interference by cybercrime actors or other parties who want to enter the system without having access rights. From the research, the analysis of the performance of the access control list using the zone based policy firewall method, it was found that the application of zone-based policy firewall computer network security was able to limit access to the server from clients connected to the same network. The zone-based policy firewall is also able to hide the hop count that is passed to connect the client to the server.

Penulis Korespondensi:

Firmansyah,
Program Studi Sistem Informasi,
Sekolah Tinggi Manajemen Informatika dan Komputer Nusa Mandiri,
Email: firmansyah.fmy@nusamandiri.ac.id

1. PENDAHULUAN

Perkembangan teknologi jaringan komputer setiap harinya selalu mengalami peningkatan dan pembaharuan, hal ini dapat menyebabkan potensi terjadinya ancaman di dalam dunia internet [1]. Berdasarkan data yang didapatkan dari APJII (Asosiasi Penyelenggara Jasa Internet Indonesia) pengguna layanan internet di Indonesia pada tahun 2018 sebesar 171.176.716 dari 264.161.600 jiwa. Meskipun, jaringan inernet sudah menjadi *platform* utama di Indonesia dalam berbagai kegiatan, akan tetapi masalah keamanan dan privasi masih menjadi sebuah masalah yang seringkali muncul terutama dalam transaksi elektronik [2]. Semakin bertumbuhnya pengunalayanan internet di Indonesia akan berbanding lurus dengan kerentanan dari sebuah data. Hal ini akan berpotensi terjadinya kelemahan dari sistem keamanan data didalam jaringan internet. Kejahatan didalam dunia maya telah menjadi sebuah anacaman serius seiring pesatnya pertumbuhan internet di Indonesia [3]. Keamanan jaringan sangatlah vital bagi sebuah jaringan komputer, kelemahan-kelemahan yang terdapat pada jaringan komputer jika tidak dilindungi dan dijaga dengan baik akan menyebabkan sebuah kerugian [4] . Bahkan, sistem keamanan jaringan komputer beberapa tahun ini menjadi sebuah fokus utama dalam dunia jaringan komputer, hal ini disebabkan tingginya ancaman dan serangan dari internet.

Kejahatan didalam jaringan internet atau *Cybercrime* sulit untuk dideteksi, dikarenakan para pelaku memiliki banyak waktu untuk melarikan diri dari lokasi mereka dalam melakukan kejahatan tersebut [4]. Marak terjadinya kasus *Cybercrime* belakangan ini, menjadi sebuah kecemasan bagi pengguna layanan internet terutama bagi perusahaan yang memiliki data *center* yang dapat diakses melalui internet [5]. Sebuah keamanan jaringan komputer harus mempertimbangkan akses kenyamanan dan keamanan yang digunakan [6]. Manajemen *firewall* dapat memfasilitasi keamanan hanya untuk wilayah atau *security policy* tertentu saja yang akan dapat melakukan akses metode dasar adalah dengan menggunakan *firewall* tunggal yang menjadi penyangga jaringan *internal* dan *external* [7].

Pengimplementasian keamanan jaringan menggunakan metode *zone-based policy firewall* diharapkan mampu meminimalisir terjadinya kebocoran data. *Zone-based police* merupakan sebuah motode dari *Access Control List* (ACL) merupakan penyataan perizinan atau penolakan yang diterapkan pada sebuah alamat jaringan atau pada lapisan protokol dan ACL dapat digunakan untuk menentukan akses dari keluar masuknya sebuah paket didalam jaringan sedangkan *frame relay* merupakan teknologi yang menghandalkan *frame-frame* yang diteruskan untuk melakukan pengiriman paket data [8], dan dimana *frame* adalah sebuah paket data [9]. *Zone-based policy firewall* menggunakan mekanisme keamanan yang digunakan untuk melindungi sistem internal dari gangguan para pelaku *Cybercrime* atau pihak-pihak lain yang ingin memasuki kedalam sistem tanpa mempunyai hak akses. Teknik-teknik sistem keamanan jaringan dan pencegahan terhadap serangan pada sistem informasi perlu dikembangkan sehingga *integrity*, *availability* dan *confidentiality* [10][11]. Salah satunya adalah dengan cara membangun sistem keamanan jaringan dan sistem pencegahan serangan yaitu dengan pengimplementasian Z*one-based policy firewall* menyediakan keamanan berbasis zona yang memungkinkan kebijakan layanan berdasarkan zona yang sama walaupun berbeda *interface* pada router. Terdapat dua fitur yang harus diaktifkan untuk dapat berkomunikasi dengan *zone-based policy firewall* yaitu nama zona yang digunakan dan manajemen zona yang ditetapkan [12]. *Interface* pengguna memungkinkan pengguna layanan untuk mementukan zona dan kebijakan secara berbeda dari keamanan virtual. Serta, lalu lintas antar zona akan dibatasi oleh *firewall* sesuai dengan kebijakan *access control policy* [13].

Pada penelitian sebelumnya, implementasi teknik *Demilitarized Zone* (DMZ) pada layanan server jaringan *Local Area Network* (LAN) dapat melakukan *filter* terhadap serangan DoS jenis *Internet Control Message* Protocol (ICMP) *flooding attack* dan *User Datagram Protocol* (UDP) *flooding attack* [13]. Pada penelitian lainnya, terbentuknya koneksi antar jaringan dalam topologi beserta suksesnya fungsi dari firewall dan bekerjanya *rule* untuk area DMZ. Keberhasilan dalam pengaplikasian diuji kembali dengan melakukan beberapa metode serangan yang akan ditanggulangi oleh konfigurasi yang telah diterapkan pada alat jaringan beserta server [14]. Sedangkan pada penelitian lainnya pula, *firewall* DMZ bekerja untuk membuat semua paket yang akan masuk dan keluar jaringan harus melalui suricata, sehingga suricata akan memeriksa paket tersebut dan ketika ada paket yang termasuk dalam paket yang dicurigai oleh suricata, *firewall* mikrotik akan mengambil alih untuk melakukan tindakan pada paket tersebut [15]. Diharapkan dengan pengimplementasian *Zone-based policy firewall* mampu meminimalisir kejahatan didalam dunia jaringan komputer dikarenakan telah dilakukannya pembatasan hak akses berdasarkan zona-zona yang telah ditentunkan. Serta pengimplementasian *Zone-based policy firewall* mampu mempermudah didalam manajemen suatu keamanan jaringan.

2. METODE PENELITIAN

Dalam penelitian jaringan *Zone-Base Policy Firewall* peneliti menggunakan bantuan *software* Cisco *Packet Tracer Version*: 7.0.0.0305 untuk membuat simulasi jaringan komputer namun tidak mengurangi dan tidak merubah fitur seperti *device* aslinya. Untuk melakukan penelitian *Zone-Base Policy Firewall* peneliti menggunakan tiga (3) perangkat router series Cisco1941/K9 dengan Cisco IOS *Software version* 15.1(4) M4 serta mengaktifkan *Security Technology Package* yang dapat terlihat pada gambar 1. Untuk mengetahui performa dari pengimplementasian *Zone-based policy firewall* peneliti melakukan pengujian berdasarkan sebelum dan setelah pengimplementasian *Zone-based policy firewall* dengan melakukan pengiriman paket data dari zona yang berbeda.

```
Technology Package License Information for Module:'c1900'

----------------------------------------------------------------
Technology    Technology-package          Technology-package
              Current       Type          Next reboot
----------------------------------------------------------------
ipbase        ipbasek9      Permanent     ipbasek9
security      securityk9    Evaluation    securityk9
data          disable       None          None
```

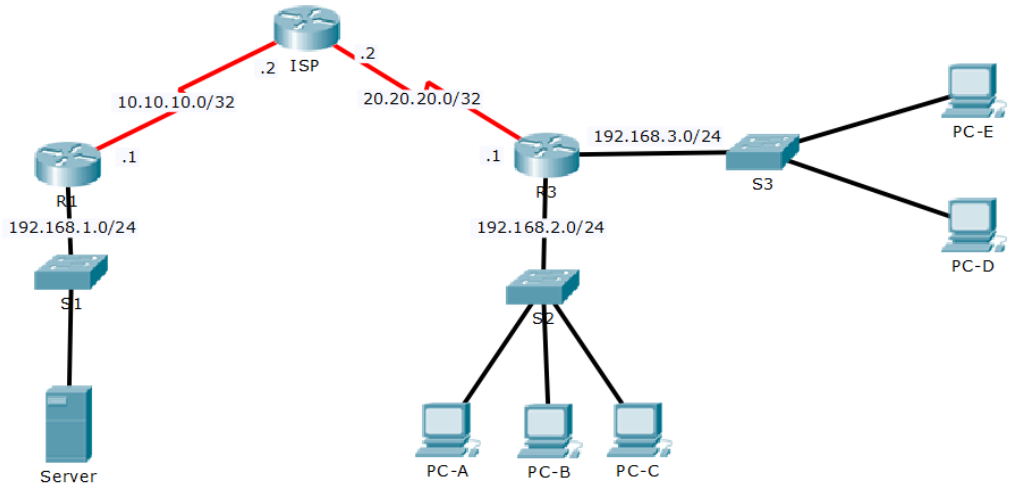
Gambar 1. *Technology-package securityk9*

Metode penelitian yang digunakan dalam penelitian ini menggunakan *The Security Policy Development Life Cycle (*SPDLC), yang memiliki enam (6) tahapan, yaitu:

1. Identifikasi
   Identifikasi digunakan untuk melakukan pengidentifikasian terhadap permasalahan keamanan didalam jaringan komputer.
2. Analisis
   Pada tahapan ini penulis melakukan percobaan untuk mengetahui resiko dan ancaman didalam keamanan jaringan sebelum dan sesudah pengimplementasian *Firewall Base Policy*.
3. Perancangan
   Tahapan ini penulis melakukan perancangan keamanan jaringan *Firewall Base Policy*.
4. Implementasi
   Pada tahapan ini penulis melakukan konfigurasi *Firewall Base Policy* dan melakukan tahapan uji konektifitas terhadap keamanan jaringan.
5. Audit
   Tahap audit digunakan untuk melakukan pemeriksaan terhadap system keamanan yang telah diimplementasikan.
6. Evaluasi
   Tahapan evaluasi digunakan untuk melakukan evalusi *system* keamanan yang telah diterapkan.

3. HASIL DAN ANALISIS

Terlihat pada gambar 2 skema jaringan yang digunakan dalam pengimplementasikan jaringan berbasis *Zone-Base Policy Firewall*. Terdapat 1 (Satu) perangkat *server* yang terkoneksi dengan jaringan lokal R1. Pengimplementasian *Zone-Base Policy Firewall* akan memberikan batasan akses dan limitasi menuju *server* berdasarkan kesamaan zona. Hak akses menuju server hanya dapat dilakukan oleh jaringan yang berada pada R3 dengan menggunakan *network* 192.168.3.0/24 dan tidak diizinkan untuk melakukan akses menuju *server* untuk *network* 192.168.2.0/24. Namun, *network* 192.168.2.0/24 dengan *network* 192.168.3.0/24 tetap dapat saling berkomunikasi satu dengan lainnya.



Gambar 2. Skema Jaringan

Skenario pengujian akan melakukan percobaan akses dari *client* dengan *network* 192.168.2.0/24 dan *client* dengan *network* 192.168.3.0/24 menuju ke *server*. Lalu, melakukan pengujian dari sisi *server* menuju ke *network* yang digunakan *client* serta melakukan uji konektifitas dari sisi *client* menuju *client* lainnya yang berada didalam *network* yang berbeda.

Tabel 1. Spesifikasi IP *Address*

Device	*Interface*	IPv4	*Gateway*
ISP	Se0/0/0	10.10.10.2	-
	Se0/0/1	20.20.20.2	-
R1	Se0/0/0	10.10.10.1	-
	G0/0	192.168.1.1	-
R3	Se0/0/1	20.20.20.1	-
	G0/0	192.168.2.1	-
	G0/1	192.168.3.1	-
Server	NIC	192.168.1.2	192.168.1.1
PC-A	NIC	192.168.2.2	192.168.2.1
PC-B	NIC	192.168.2.3	
PC-C	NIC	192.168.2.4	
PC-D	NIC	192.168.3.2	192.168.3.1
PC-E	NIC	192.168.3.3	

Dijelaskan pada Tabel 1 merupakan spesifikasi IP *Address* yang digunakan dalam pengimplementasian jaringan *Zone-Base Policy Firewall*. R1 menggunakan *interface* Se0/0/0 untuk terhubung dengan ISP dengan alokasi IP *Address* 10.10.10.1/24 dan *interface* G0/0 dengan alokasi IP Address 192.168.1.1/24 yang digunakan untuk menghubungkan jaringan lokal. Sedangkan, *interface* pada R3 yang terhubung dengan ISP adalah *inteface* Se0/0/1 dengan alokasi IP Address 20.20.20.1/24 dan *interface* G0/0 digunakan untuk jaringan lokal dengan alokasi IP *Address* 192.168.2.1/24 serta *interface* G0/1 dengan alokasi IP *Address* 192.168.3.1/24.

3.1 Konfigurasi *Static Routing*

Untuk mendukung pengimplementasian jaringan *Zone-Base Policy Firewall* sesuai dengan skema jaringan yang digunakan pada gambar 1. Penerapan static routing diperlukan untuk membentuk *end to end* antara IP *Address* yang menghubungkan *router* dengan *router* secara langsung. Konfigurasi *static routing* yang digunakan terhadap R1 adalah:

R1 (config)#ip route 0.0.0.0 0.0.0.0 10.10.10.2

Pengimplementasian static route haruslah mempertimbangkan dan memperhatikan alokasi IP *Address* yang digunakan seperti yang tertera pada Tabel 1 serta memastikan alokasi IP *Address* tersebut sudah diimplementasikan didalam R1 maupun R3. R3 tidaklah luput dari konfigurasi *static routing* untuk mendukung suksesnya pengimplementasian jaringan *Zone-Base Policy Firewall*. Konfigurasi static routing yang digunakan terhadap R3 adalah:

R3(config)# ip route 0.0.0.0 0.0.0.0 20.20.20.2

Konfigurasi *static routing* haruslah memperhatikan IP *Address* dari *Next-Hop* atau *Neighbour* didalam jaringan yang digunakan.

3.2 Uji Konektifitas Jaringan Sebelum Penerapan *Zone-Base Policy Firewall*

Sebelum diimplementasikannya keamanan jaringan menggunakan metode *Zone-Base Policy Firewall*, semua *client* yang terkoneksi didalam jaringan dapat berkomunikasi dengan *server* tanpa adanya batasan akses diantara *server* dengan *client*. Dijelaskan pada gambar 3 merupakan hasil *traceroute* dari *client* dengan *network* 192.168.2.0 menuju ke *server* dengan memiliki 4 *hop-count* dengan melalui gateway 192.168.2.1 menuju 20.20.20.2 menuju ke 10.10.10 hingga sampai pada *server*.

```
C:\>tracert 192.168.1.2

Tracing route to 192.168.1.2 over a maximum of 30 hops:

  1    16 ms     0 ms      0 ms      192.168.2.1
  2    11 ms     11 ms     1 ms      20.20.20.2
  3    0 ms      11 ms     13 ms     10.10.10.1
  4    11 ms     12 ms     13 ms     192.168.1.2

Trace complete.
```

Gambar 3. Tracer 192.168.2.0 menuju *Server*

Sedangkan dijelaskan pada gambar 4, merupakan uji konektifitas dari *client* dengan *network* 192.168.3.0 menuju ke *server*. Terlihat *hop-count* yang pertama dilalui oleh *client* adalah *gateway* dengan alokasi IP *Address* 192.168.3.1 lalu menuju 20.20.20.2 menuju ke 10.10.10 hingga sampai pada *server*, serta lalu lintas *tranfer* paket data dari *client* menuju ke *server* dapat berjalan dengan baik.

```
C:\>tracert 192.168.1.2

Tracing route to 192.168.1.2 over a maximum of 30 hops:

  1    0 ms      0 ms      0 ms      192.168.3.1
  2    0 ms      0 ms      0 ms      20.20.20.2
  3    0 ms      2 ms      2 ms      10.10.10.1
  4    12 ms     1 ms      0 ms      192.168.1.2

Trace complete.
```

Gambar 4**.** Tracer 192.168.3.0 menuju *Server*

3.3 Konfigurasi *Zone-Base Policy Firewall*

Security Technology package sangatlah berperan penting dalam pengimplementasian *Zone-Base Policy Firewall* dikarenakan jika tidak mengaktifkan *technology-package* akan berdampak tidak dapat diimplementasikannya *Zone-Base Policy Firewall*. Terlihat pada gambar 5 sebelum pengaktifan *Technology-package* pada Cisco IOS.

```
Technology Package License Information for Module:'c1900'

-----------------------------------------------------------------
Technology    Technology-package          Technology-package
              Current       Type          Next reboot
-----------------------------------------------------------------
ipbase        ipbasek9      Permanent     ipbasek9
security      disable       None          None
data          disable       None          None
```

Gambar 5. Sebelum Pengaktifan *Technology-package*

Untuk mengaktifkan *Technology-package* pada Cisco IOS dapat menggunakan konfigurasi:

R3(config)#license boot module c1900 technology-package securityk9

Konfigurasi tersebut dapat digunakan untuk mengaktifkan *Technology-package* dan hasil dari pengaktifan *Technology-package* terlihat pada gambar 6.

```
Technology Package License Information for Module:'c1900'

-----------------------------------------------------------------
Technology    Technology-package          Technology-package
              Current       Type          Next reboot
-----------------------------------------------------------------
ipbase        ipbasek9      Permanent     ipbasek9
security      securityk9    Evaluation    securityk9
data          disable       None          None
```

Gambar 6. Setelah Pengaktifan *Technology-package*

Setelah mengaktifkan fitur *securityk9* langkah selanjutnya mengaktifkan zona yang akan digunakan, baik zona *internal* maupun zona *external* serta pengimplementasian *access control list* pada R3. Konfigurasi pengaktifan zona dan *Access Control List* (ACL) hanya dilakukan pada R3 dengan menggunakan perintah:

R3(config)#zone security Z-INSIDE
R3(config)#zone security Z-OUTSIDE
R3(config)#access-list 101 permit ip 192.168.3.0 0.0.0.255 any
R3(config)#class-map type inspect match-all INSIDE-PROTOCOL
R3(config-cmap)#match access-group 101

Pembatasan akses menggunakan *access-list* bermaksud untuk membatasi akses hanya dapat dilalui dan diizinkan oleh *network* 192.168.3.0/24 saja. Metode yang digunakan dalam pengimplementasian *Zone-Base Policy Firewall* menggunakan *Inspect* untuk mengamanakan secara *privasi* antara *Source Member Zone* dengan *Destination Member Zone*. Maka akses dari alamat selain *Member Zone* tersebut akan terblok aksesnya. Untuk pengimplementasian *Zone-Base Policy Firewall* penggunaan ACL tidaklah sebatas *permit* dan *deny*. Namun, menggunakan *firewall policy* yang lebih spesifik untuk menentukan *matched* terhadap *traffic* yang akan diamankan.

R3(config)#policy-map type inspect INSIDE-TO-OUTSIDE
R3(config-pmap)#class type inspect INSIDE-PROTOCOL
R3(config-pmap-c)#inspect

R3(config)#zone-pair security INSIDE-TO-OUTSIDE-Z source Z-INSIDE destination Z-OUTSIDE
R3(config-sec-zone-pair)#service-policy type inspect INSIDE-TO-OUTSIDE

3.4 Uji Konektifitas Jaringan Dengan *Zone-Base Policy Firewall*-1

Uji konektifitas yang pertama kali dilakukan adalah memastikan fungsional dari pengimplementasian zona *inside* yang digunakan pada jaringan lokal R3. Pengujian kinerja jaringan dapat dilakukan dengan cara melakukan pengiriman paket ICMP dari jaringan local *client* menuju *Server*. Terlihat pada gambar 7 merupakan hasil pengujian konektifitas paket ICMP dari *client* yang menggunakan *network* 192.168.3.0 berstatus sukses yang artinya jaringan dapat berjalan dengan baik.

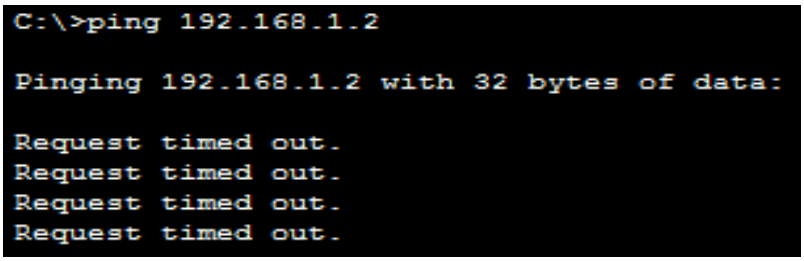
```
C:\>ping 192.168.1.2

Pinging 192.168.1.2 with 32 bytes of data:

Reply from 192.168.1.2: bytes=32 time=14ms TTL=125
Reply from 192.168.1.2: bytes=32 time=12ms TTL=125
Reply from 192.168.1.2: bytes=32 time=14ms TTL=125
Reply from 192.168.1.2: bytes=32 time=12ms TTL=125
```

Gambar 7. Pengujian ICMP dari *Network* 192.168.3.0

Sedangkan, pengujian yang dilakukan dari sisi *client* dengan *network* 192.168.2.0 menuju ke *server* berstatus *Request timed out*, terlihat pada gambar 8. Hal ini terjadi dikarenakan telah diimplementasikannya *Zone-Base Policy Firewall* yang mampu melakukan pembatasan akses *client* menuju ke *server* hanya dapat dilalui oleh *network* 192.168.3.0



Gambar 8. Pengujian ICMP dari *Network* 192.168.2.0

Dijelaskan pada gambar 9 merupakan *policy map* yang didapatkan pada R3. *Policy map akan* memberikan informasi *log traffic* didalam lalu lintas router dengan memberikan *note Service-policy inspect*: *INSIDE-TO-OUTSIDE* sesuai dengan pengimplementasian. Terlihat *session* 390434776 dengan IP *Address* 192.168.3.3:50 melakukan akses menuju 192.168.1.2:0 dengan menggunakan paket ICMP dan dengan status pengiriman paket ICMP dari *client Drop*.

```
R3#sh policy-map type inspect zone-pair sessions

policy exists on zp INSIDE-TO-OUTSIDE-Z
 Zone-pair: INSIDE-TO-OUTSIDE-Z

  Service-policy inspect : INSIDE-TO-OUTSIDE

    Class-map: INSIDE-PROTOCOL (match-all)
      Match: access-group 101
      Inspect

        Number of Established Sessions = 1
        Established Sessions
         Session 390434776 (192.168.3.3:50)=>(192.168.1.2:0) icmp SIS_OPEN
          Created 00:00:01, Last heard 00:00:01
           ECHO request
          Bytes sent (initiator:responder) [28:28]
    Class-map: class-default (match-any)
      Match: any
      Drop (default action)
        0 packets, 0 bytes
```

Gambar 9. *Policy Map* ICMP

3.5 Uji Konektifitas Jaringan Dengan *Zone-Base Policy Firewall*-2

Pengujian yang kedua adalah melakukan uji konektifitas terhadap akses HTTP menuju *server* dari sisi *client* yang menggunakan *network* 192.168.3.0. Terlihat pada gambar 10 merupakan hasil *policy map* yang didapatkan ketika terdapat zona yang sama melakukan akses menuju ke *server*.

```
R3#sh policy-map type inspect zone-pair sessions

policy exists on zp INSIDE-TO-OUTSIDE-Z
 Zone-pair: INSIDE-TO-OUTSIDE-Z

  Service-policy inspect : INSIDE-TO-OUTSIDE

    Class-map: INSIDE-PROTOCOL (match-all)
      Match: access-group 101
      Inspect

        Number of Established Sessions = 1
        Established Sessions
         Session 470211024 (192.168.3.3:1025)=>(192.168.1.2:80) tcp SIS_OPEN/TCP_ESTAB
          Created 00:00:03, Last heard  00:00:02
          Bytes sent (initiator:responder) [284:575]
    Class-map: class-default (match-any)
      Match: any
      Drop (default action)
        0 packets, 0 bytes
```

Gambar 10. *Policy Map* HTTP

3.6 Uji Konektifitas Jaringan Dengan *Zone-Base Policy Firewall*-3

Pengujian yang ketiga pada jaringan *Zone-Base Policy Firewall* adalah melakukan uji konektifitas secara menyeluruh seperti yang terlihat pada tabel 2.

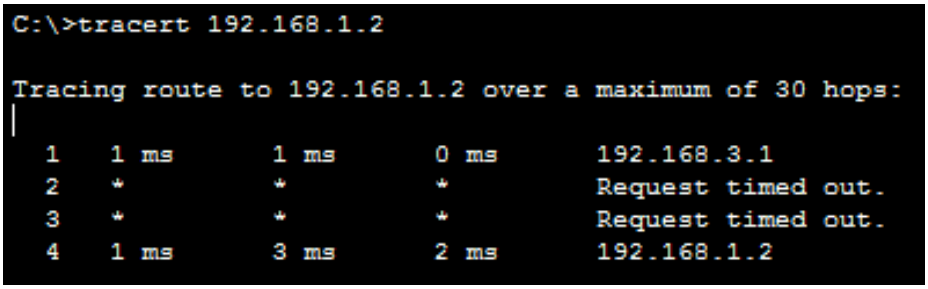
Tabel 2. Uji Konektifitas Jaringan *Zone-Base Policy Firewall*

Source	*Destination*	*Protocol*	Status
192.168.2.0	192.168.3.0	ICMP	*Success*
192.168.2.0	*Server*	ICMP	*Request Timed Out*
192.168.2.0	*Server*	HTTP	*Request Timed Out*
192.168.3.0	192.168.2.0	ICMP	*Success*
192.168.3.0	*Server*	ICMP	*Success*
192.168.3.0	*Server*	HTTP	*Success*
Server	192.168.2.0	ICMP	*Request Timed Out*
Server	192.168.3.0	ICMP	*Request Timed Out*

Tabel 2 menjelaskan bahwa *client* dengan network 192.168.2.0 hanya dapat melakukan konektifitas terhadap *client* dengan *network* 192.168.3.0 dan tidak dapat melakukan akses terhadap *server* baik menggunakan protokol ICMP maupun HTTP. Sedangkan *client* dengan *network* 192.168.3.0 mampu melakukan akses terhadap keseluruhan jaringan berjalan baik untuk berkomunikasi antara *client* maupun berkomunikasi dengan *server*. Dan dari sisi *server* tidak dapat melakukan komunikasi menuju *client* dengan *network* 192.168.2.0 dan *client* dengan *network* 192.168.3.0.

3.7 Uji Konektifitas Jaringan Dengan *Zone-Base Policy Firewall*-4

Keamanan jaringan komputer menggunakan metode *Zone-Base Policy Firewall* mampu menyembunyikan *hop count* yang dilalui, terlihat pada gambar 11. *Tracert* yang dilalui dari *client* dengan *network* 192.168.3.0 menuju ke *server* hanya menampilkan alokasi *gateway* dari *source* dan *destination* tanpa memberikan informasi dari *hop count* yang dilaluinya.



Gambar 11. Tracert *Network* 192.168.3.0

4. KESIMPULAN

Penerapan keamanan jaringan menggunakan metode *Zone-Base Policy Firewall* mampu meminimalisir terjadinya kebocoran data yang bersifat pribadi dan sangat rahasia. Dikarenakan sistem keamanan yang digunakan pada *Zone-Base Policy Firewall* melakukan pembatasan akses berdasarkan zona yang sama dengan melakukan pertimbangan nama zona dan manajemen zona yang digunakan. Ketika terdapat pengguna yang mencoba melakukan akses kedalam jaringan yang diamankan maka akses tidak akan diizinkan dikarenakan. Pengimplementasian *Zone-Base Policy Firewall* mampu menyingkat penggunaan *access control list* serta lebih mempermudah dalam melakukan maintenance didalam jaringan. Dari hasil penelitian didapatkan *server* hanya dapat diakses dari *client* dengan zona yang sama atau *client* dengan *network* 192.168.3.0. Serta *Zone-based policy firewall* mampu menyamarkan *hop count* didalam jaringan guna meningkatkan keamanan lalu lintas transfer paket data.

REFERENSI

[1] F. Firmansyah, M. Wahyudi, and R. A. Purnama, "Analisis Performa Site to Site IP Security Virtual Private Network (VPN) Menggunakan Algoritma Enkripsi ISAKMP," *JUITA Jurnal Informatika*, vol. 7, no. 2, pp. 129-135, 2019.

[2] B. Sugiantoro, "Analisa Usabilitas Sistem Deteksi Akses Pornografi Pengguna Internet Menggunakan Metode Mccall'S," *JOIN Jurnal Online Informatika*, vol. 2, no. 1, pp. 56-61, 2017.

[3] M. Irfan, M. A. Ramdhani, W. Darmalaksana, A. Wahana, and R. G. Utomo, "Analyzes of cybercrime expansion in Indonesia and preventive actions," *IOP Conference Series Matererials Science and Engineering*, vol. 434, no. 1, pp. 1–7, 2018.

[4] I. Anugrah and R. H. Rahmanto, "Sistem Keamanan Jaringan Local Area Network Menggunakan Teknik De-Militarized Zone," *PIKSEL Peneliti Ilmu Komputer Sistem Embedded & Logic*, vol. 5, no. 2, pp. 91–106, 2018.

[5] M. Yusup, Maisyaroh, and L. Septiana, "Securing Web Application by Embedded Firewall at Gytech Indosantara Mandiri Ltd.," *PIKSEL Peneliti Ilmu Komputer Sistem Embedded & Logic*, vol. 8, no. 1, pp. 49–58, 2020.

[6] B. Fachri and F. H. Harahap, "Simulasi Penggunaan Intrusion Detection System (IDS) Sebagai Keamanan Jaringan dan Komputer," *Jurnak Media Informatika Budidarma*, vol. 4, no. 2, pp. 413–420, 2020.

[7] C. E. Suharyanto, "Analisis Penggunaan Access Control List (Acl) Dalam Jaringan Komputer Di Kawasan Batamindo Industrial Park Batam," *Jurnal Informatin System Development*, vol. 2, no. 2, pp. 122–128, 2019.

[8] R. Novrianda, "Simulasi Teknologi Frame Relay Pada Jaringan Vpn Menggunakan Cisco Packet Tracer the Simulation of Frame Relay Methods on Vpn Networks Using Cisco Packet Tracer," *Jurnal Digital*, vol. 1, no. 1, pp. 45–55, 2018.

[9] H. Supendar and Y. Handrianto, "Teknik Frame Relay Dalam Membangun Wide Area Network Dengan Metode Network Development Life Cycle," *Bina Insani. ICT Journal*, vol. 4, no. 2, pp. 121–130, 2017.

[10] S. Arlis, "Analisis Firewall Demilitarized Zone Dan Switch Port Security Pada Jaringan," *Jurnal KomtekInfo (Komput. Teknol. Inf.)*, vol. 6, no. 1, pp. 29–39, 2019.

[11] B. M. Sukhovilov and E. A. Grigorova, "Development of System for Protecting IT Environment of Enterprise Based on Demilitarized Zone Concept Using Virtualization Technology," in *Proceedings - 2018 Global Smart Industry Conference, GloSIC 2018*, 2018, pp. 1–6.

[12] K. Demertzis and L. Iliadis, "Cognitive Web Application Firewall to Critical Infrastructures Protection from Phishing Attacks," *Journal of Computations & Modelling*, vol. 9, no. 2, pp. 1792–8850, 2019.

[13] R. Vanickis, P. Jacob, S. Dehghanzadeh, and B. Lee, "Access Control Policy Enforcement for Zero-Trust-Networking," *29th Irish Signals Systems Conference ISSC 2018*, vol. 1, no. 2, pp. 1–6, 2018.

[14] K. Kurniati and R. N. Dasmen, "The Simulation of Access Control List (ACLs) Network Security for Frame Relay Network at PT. KAI Palembang," *Lontar Komputer Jurnal Ilmiah Teknologi Informasi*, vol. 10, no. 1, pp. 49-61, 2019.

[15] Firmansyah, S. Dewi, and R. adi Purnama, "Quality Of Service Gateway Load Balancing Protocol Message Digest Algorithm 5 Authentication Untuk Peningkatan Kualitas Jaringan," *Jurnal Teknik Informatika*, vol. 5, no. November, pp. 45–50, 2020.