Jurnal Ilmu Teknik dan Komputer
Vol. 5 No. 2 Juli 2021
ISSN 2548-740X
E-ISSN 2621-1491

Konfigurasi Cicso ASA Firewall Menggunakan ASDM

Ananta Kwarta Durianto*, Djuniadi**

*Jurusan Ilmu Komputer, Fakultas Matematika dan Ilmu Pengetahuan Alam, Universitas Negeri Semarang
Sekaran, Kec. Gunungpati, Kota Semarang, Jawa Tengah 50229
anantakwarta@students.unnes.ac.id

**Jurusan Teknik Elektro, Fakultas Teknik, Universitas Negeri Semarang
Sekaran, Kec. Gunungpati, Kota Semarang, Jawa Tengah 50229
djuniadi@mail.unnes.ac.id

ABSTRACT

Cisco Adaptive Security Appliance *(ASA) adalah perangkat keamanan jaringan tingkat lanjut yang mengintegrasikan* firewall stateful, *VPN, dan kemampuan lainnya. ASA digunakan untuk membuat* firewall *dan melindungi jaringan internal perusahaan dari penyusup eksternal sambil mengizinkan host internal mengakses Internet. ASA menciptakan tiga antarmuka keamanan: Luar, Dalam, dan DMZ. Ini memberi pengguna luar akses terbatas ke DMZ dan tidak ada akses ke sumber daya internal. Pengguna dalam dapat mengakses DMZ dan sumber daya luar. Metode yang digunakan pada artikel ini adalah* Adaptive Security Device Manager *(ASDM). Hasil dari simulasi Firewall di atas yaitu bahwa PC-B dapat mengakses DMZ server. DMZ server tidak dapat mengakses PC-B.*

Kata Kunci: ASA, firewall, Packet Tracer, ASDM

PENDAHULUAN

Internet adalah hal yang umum digunakan untuk menghubungkan dunia. Namun, kurangnya jaminan keamanan dalam hal pertukaran informasi. Karena alasan keamanan, kerahasiaan, integritas dan ketersediaan data menjadi faktor penting yang perlu diperhatikan. Oleh karena itu, banyak solusi keamanan yang telah disediakan untuk mengamankan pertukaran informasi melalui Internet (Dwi Ely Kurniawan, 2019).

Keamanan infrastruktur jaringan telah menjadi prioritas utama bagi organisasi mana pun. Di antara solusi keamanan multilayer yang tersedia untuk infrastruktur jaringan, lapisan *firewall* adalah salah satu pertahanan tertua dan utama untuk jaringan apa pun. Firewall adalah perangkat keras atau perangkat lunak yang melindungi komputer dan jaringan dari lalu lintas jaringan yang tidak diinginkan dan mencegah pengguna Internet yang tidak berwenang mengakses jaringan pribadi (Trabelsi & Saleous 2019). *Firewall* memonitor lalu lintas jaringan dan mengizinkan atau menolak lalu lintas tertentu berdasarkan seperangkat aturannya. Cisco Adaptive Security Appliance (ASA) 5505 Series Firewall adalah salah satu *firewall* paling populer dan canggih secara teknis untuk mengamankan jaringan dan sistem organisasi. Cisco Adaptive Security Appliance (ASA) Firewall mampu memantau dan memperingatkan berbagai ancaman umum, dengan membuat garis dasar *traffic* jaringan dan menganalisis statistik paket yang jatuh (Naik, N. et al, 2019). Ini mencakup beberapa fitur antivirus, *Intrusion Prevention System* (IPS) dan *Virtual Personal Network* (VPN) (N Naik, 2018). Cisco ASA Firewall ini dapat disimulasikan menggunakan

Cisco Packet Tracer. Cisco Packet Tracer dapat melakukan simulasi data mengenai jaringan sehingga dapat mengetahui informasi tentang keadaan koneksi suatu komputer dalam jaringan (Mufadhol, 2012; Tarkaa, 2017).

Adaptive Security Device Manager (ASDM) adalah alat konfigurasi yang disertakan dengan ASA. Alat ini memiliki antarmuka manajemen berbasis web yang mudah digunakan dan memungkinkan administrator jaringan untuk dengan cepat mengkonfigurasi, memantau, dan memecahkan masalah peralatan *firewall Cisco* (N Naik, 2018).

STUDI LITERATUR

A. Jaringan Komputer

Sekumpulan perangkat keras (*hardware*) dan perangkat lunak (*software*) dari beberapa komputer yang saling terhubung satu sama lain (Pratama, 2015). Firewall adalah perangkat keras atau perangkat lunak yang melindungi komputer dan jaringan dari lalu lintas jaringan yang tidak diinginkan dan mencegah pengguna Internet yang tidak berwenang mengakses jaringan pribadi (. Tujuan dari jaringan komputer adalah agar dapat mencapai tujuannya, setiap bagian dari jaringan komputer dapat meminta dan memberikan layanan (*service*). Pihak yang meminta/menerima layanan disebut klien (*client*) dan yang memberikan/mengirim layanan disebut peladen (*server*). Desain ini disebut dengan sistem *client-server*, dan digunakan pada hamper seluruh aplikasi jaringan komputer (Yudianto, 2014).

B. Firewall

Firewall adalah sebuah sistem atau kelompok sistem yang menerapkan sebuah *access control policy* terhadap lalu lintas jaringan yang melewati titik-titik akses dalam jaringan (Imam, 2011). Firewall bertugas untuk memastikan izin akses dari lingkupannya. Sekarang ini firewall semakin menjadi fungsi standar yang ditambahkan untuk semua host yang berhubungan dengan network (Purbo, 2000).

Fungsi umum dari *firewall* antara lain:

a. *Static packet filtering*
b. *Dynamic packet filtering*
c. *Stateful filtering*
d. *Proxy*

C. Cisco ASA 5505 Series Firewall

Cisco ASA (*Adaptive Security Appliance*) 5505 Series memberikan solusi yang dirancang khusus untuk keamanan tertinggi dan layanan VPN terbaik. Dengan arsitektur layanan terukur yang inovatif, ini adalah komponen inti dari Cisco SelfDefending Network. Cisco ASA 5505 Series dapat memberikan pertahanan ancaman proaktif, kontrol aktivitas jaringan, dan kontrol lalu lintas aplikasi. Ini juga memberikan koneksi VPN yang fleksibel. Model yang lebih rendah tidak hanya untuk perlindungan rumah kantor atau kantor cabang tetapi juga dapat melindungi perusahaan kecil dan menengah. Model yang lebih tinggi dapat melindungi jaringan perusahaan besar dan memberi mereka perlindungan keamanan yang mendalam. Ini dapat mengurangi biaya penerapan secara keseluruhan dan kompleksitas pengoperasian (Xu, J. & Su, W., 2013).

Rangkaian pengelolaan dan pemantauan Cisco memungkinkan penerapan dan pengoperasian Cisco ASA 5505 Series Firewall dalam skala besar. Cisco menyediakan solusi lengkap, mencakup manajemen dan pemantauan. Juga disertakan dengan solusinya adalah *Cisco Adaptive Security Device Manager* (ASDM), yang menyediakan antarmuka manajemen dan pemantauan berbasis *browser* yang kuat namun mudah digunakan untuk peralatan keamanan individu (Cisco_A, n.d.).

D. Adaptive Security Device Manager

Adaptive Security Device Manager (ASDM) adalah suatu alat manajemen *firewall* berbasis GUI yang berguna untuk mengelola Cisco ASA Firewall melalui antarmuka lokal berbasis web.

Berdasarkan Cisco System Inc. (Cisco_B, n.d.) fitur-fitur yang ada dalam ASDM meliputi:

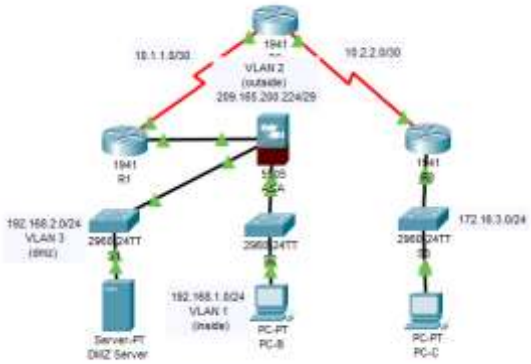
a. Setup Wizard, yang membantu untuk mengkonfigurasi dan mengelola perangkat firewall Cisco
b. Menampilkan log secara real-time dan pemantauan yang memberikan informasi mengenai status dan kesehatan alat firewall
c. Fitur troubleshooting dan debugging yang kuat seperti pelacakan paket dan penangkapan paket

METHODOLOGI

A. Desain Simulasi

Jurnal Ilmu Teknik dan Komputer
Vol. 5 No. 2 Juli 2021
ISSN 2548-740X
E-ISSN 2621-1491

Simulasi ini didesain dengan topologi standar untuk mencoba simulasi konfigurasi ASA Firewall.



Gambar 1. Desain Simulasi

Berdasarkan Gambar 1, terdapat 3 router, 3 switch, ASA Firewall 5505 dan 3 PC meliputi server DMZ, PC-B, dan PC-C. Ketiga router dihubungkan dengan kabel serial dan yang lainnya dihubungkan dengan kabel Ethernet. PC-B adalah jaringan dalam (inside), Server-PT adalah DMZ, dan PC-B ada jaringan luar (outside).

Tabel *addressing* dari topologi Gambar 1 dapat dilihat pada Tabel 1.

Tabel 1. IP Addressing

Device	Interface	IP Address	Subnet Mask	Default Gateway	Switch Port
R1	G0/0	209.165.200.226	255.255.255.248	N/A	ASA E0/0
	S0/0/0 (DCE)	10.1.1.1	255.255.255.252	N/A	N/A
R2	S0/0/0	10.1.1.2	255.255.255.252	N/A	N/A
	S0/0/1 (DCE)	10.2.2.2	255.255.255.252	N/A	N/A
R3	G0/1	172.16.3.1	255.255.255.0	N/A	S3 F0/5
	S0/0/1	10.2.2.1	255.255.255.252	N/A	N/A
ASA	VLAN 1 (E0/1)	192.168.1.1	255.255.255.0	N/A	S2 F0/24
	VLAN 2 (E0/0)	209.165.200.229	255.255.255.248	N/A	R1 G0/0
	VLAN 3 (E0/2)	192.168.2.1	255.255.255.0	N/A	S1 F0/24
PC-A	NIC	192.168.2.3	255.255.255.0	192.168.2.1	S1 F0/6
PC-B	NIC	192.168.1.3	255.255.255.0	192.168.1.1	S2 F0/18
PC-C	NIC	172.16.3.3	255.255.255.0	172.16.3.1	S3 F0/18

HASIL DAN DISKUSI

1. Konfigurasi Pengaturan Awal

a. Konfigurasi *clock rate* untuk *router* dengan kabel serial DCE yang terpasang ke *serial interface*.

```
R1 (config) # interface S0 / 0/0
R1 (config-if) # clock rate 64000
```

Sintak 1. Konfigurasi clock rate

b. Konfigurasi *static routing* pada *router*.

```
R1(config)# ip route 0.0.0.0 0.0.0.0 10.1.1.2
R3(config)# ip route 0.0.0.0 0.0.0.0 10.2.2.2
R2(config)# ip route 209.165.200.224 255.255.255.248 10.1.1.1
R2(config)# ip route 172.16.3.0 255.255.255.0 10.2.2.1
```

Sintak 2. Konfigurasi static routing

c. Konfigurasi dan enkripsi *password* pada R1

```
R1(config)# security passwords min-length 10
R1(config)# enable algorithm-type scrypt secret cisco12345
R1(config)# username admin01 privilege 15 algorithm-type scrypt secret admin01pass
R1(config)# line console 0
R1(config-line)# login local
R1(config-line)# exec-timeout 5 0
R1(config-line)# logging synchronous
R1(config)# line vty 0 4
R1(config-line)# login local
R1(config-line)# exec-timeout 5 0
R1(config-line)# logging synchronous
R1(config-line)# transport input ssh
R1(config)# ip http server
R1(config)# ip http authentication local
```

Sintak 3. Konfigurasi dan enkripsi password

d. Tes konektivitas antara PC-C dengan R1.

```
PING 209.165.200.225 (209.165.200.225) 56(84) bytes of data.
64 bytes from 209.165.200.225: icmp_seq=1 ttl=253 time=85.1 ms
64 bytes from 209.165.200.225: icmp_seq=2 ttl=253 time=34.4 ms
64 bytes from 209.165.200.225: icmp_seq=3 ttl=253 time=37.0 ms
64 bytes from 209.165.200.225: icmp_seq=4 ttl=253 time=39.9 ms
^C
--- 209.165.200.225 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3004ms
rtt min/avg/max/mdev = 34.401/49.134/85.162/20.892 ms
```

Gambar 2. Ping PC-C dengan R1

2. Konfigurasi ASA dan akses ASDM

a. Konfigurasi interface VLAN 1 untuk mempersiapkan akses ASDM.

```
ciscoasa(config)# interface vlan 1
ciscoasa(config-if)# nameif inside
INFO: Security level for "inside" set to 100 by default.
ciscoasa(config-if)# ip address 192.168.1.1 255.255.255.0
ciscoasa(config-if)# security-level 100
ciscoasa(config-if)# exit
```

Sintak 4. Konfigurasi VLAN 1

b. Aktifkan interface E0/1 menggunakan perintah no shutdown

```
ciscoasa(config)# interface e0/1
ciscoasa(config-if)# no shut
ciscoasa(config-if)# exit
```

Sintak 5. Konfigurasi interface E0/1

c. Konfigurasi interface VLAN 2

```
ciscoasa(config)# interface vlan 2
ciscoasa(config-if)# nameif outside
INFO: Security level for "outside" set to 0 by
default.
ciscoasa(config-if)# security-level 0
ciscoasa(config-if)# interface e0/0
ciscoasa(config-if)# switchport access vlan 2
ciscoasa(config-if)# no shut
ciscoasa(config-if)# exit
```

Sintak 6. Konfigurasi VLAN 2

d. Ping PC-B ke ASA VLAN 1

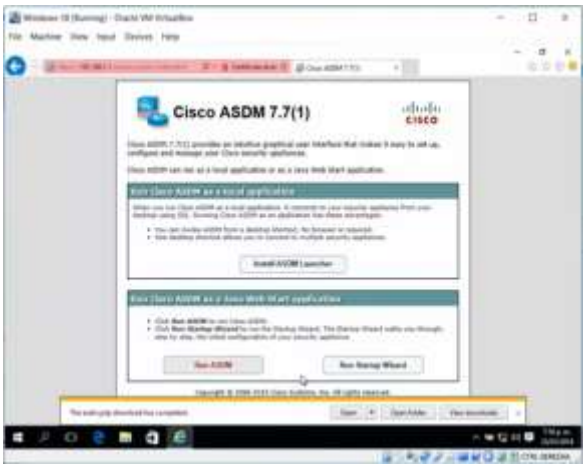
3. Konfigurasi ASDM dan verifikasi akses ke ASA
   a. Konfigurasi ASA untuk menerima koneksi HTTPS.

```
ciscoasa(config)# http server enable
ciscoasa(config)# http 192.168.1.0
255.255.255.0 inside
```

Sintak 7. Konfigurasi ASA

   b. Buka browser pada PC-B dan buka URL https://192.168.1.1

4. Akses ASDM
   Pada PC-B, akan terlihat halaman website dari ASDM. Klik Run ASDM.



Gambar 3. Halaman website ASDM

Klik OK untuk melanjutkan. ASDM akan memuat konfigurasi saat ini ke GUI.

Gambar 4. Halaman website ASDM

Gambar 5. GUI ASDM

5. Konfigurasi ASA Firewall menggunakan ASDM Startup Wizard
   a. Akses menu Configuration dan jalankan Setup Wizard.
   Pada menu bar, klik **Configuration**. Secara default akan ditampilkan **Device Setup Startup Wizard**. Klik **Launch Startup Wizard**.

Gambar 6. Tampilan menu Configuration

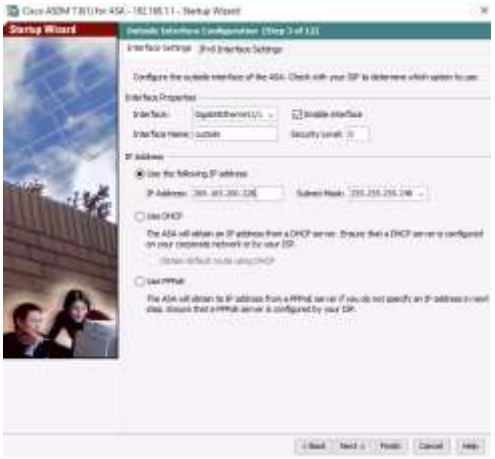
   b. Konfigurasi hostname, domain name, dan enable password.

Pada layar Startup Wizard pertama, pilih opsi **Modify Existing Configuration**, dan klik **Next** untuk melanjutkan. konfigurasikan nama host ASA **CCNAS-ASA** dan nama domain **ccnasecurity.com**. Klik kotak centang untuk mengubah sandi mode pengaktifan, ubah menjadi **cisco12345**. Setelah selesai, klik **Next** untuk melanjutkan.

Gambar 7. Tampilan Startup Wizard

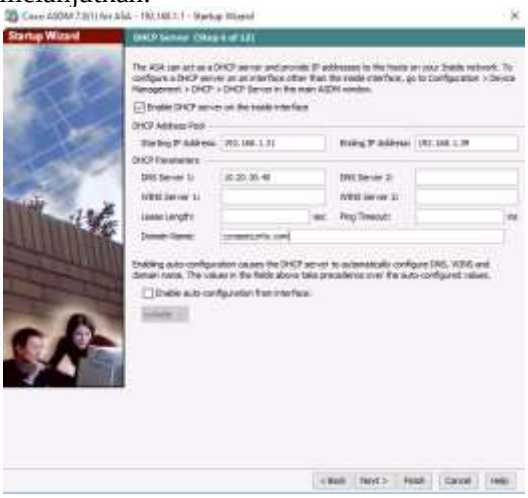
Gambar 8. Tampilan Startup Wizard

c. Konfigurasi *inside* dan *outside interface*
Interface Gi1/2 diberi nama **inside**, dan tingkat keamanan disetel ke 100 (tertinggi). Interface Gi1/1 diberi nama **outside**, dan tingkat keamanan disetel ke 0 (terendah). Klik **Next** untuk melanjutkan.



Gambar 9. Tampilan Startup Wizard

d. Konfigurasi DHCP server
Pada layar Startup Wizard Langkah 6 - Server DHCP, klik kotak centang **Enable DHCP server on the inside interface**. Masukkan Alamat IP Awal 192.168.1.31 dan Alamat IP Akhir 192.168.1.39. Masukkan alamat DNS Server 1 10.20.30.40 dan Nama Domain **ccnasecurity.com**. Klik **Next** untuk melanjutkan.

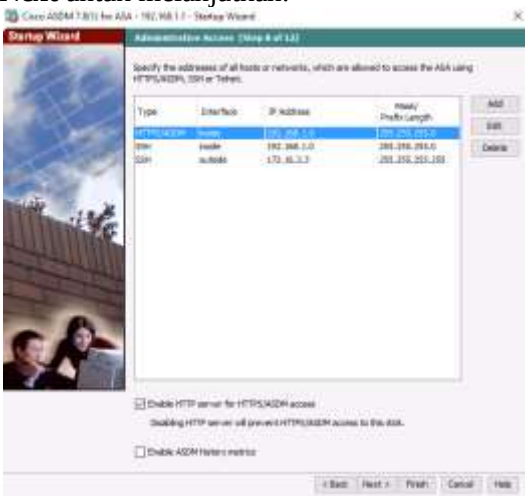


Gambar 10. Tampilan Startup Wizard

e. Pada layar Startup Wizard Langkah 7 – Port Address Translation (NAT / PAT), klik **Use Port Address Translation (PAT).** Defaultnya adalah menggunakan alamat IP dari interface outside.

Gambar 11. Tampilan Startup Wizard

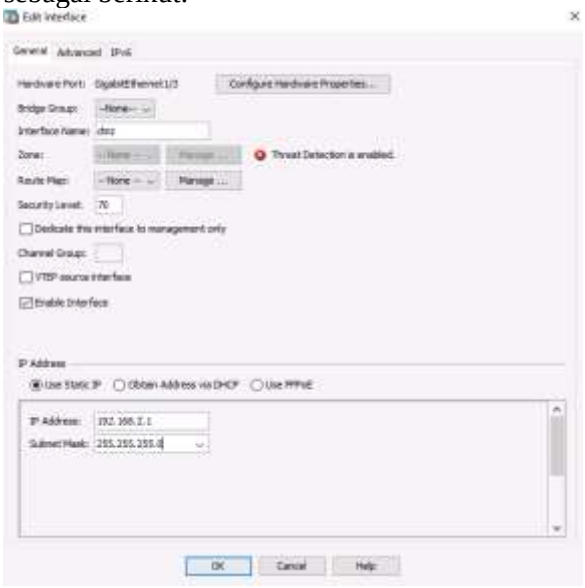
Pada layar Startup Wizard Langkah 8 – Administrative Access, akses HTTPS / ASDM saat ini dikonfigurasi untuk host di dalam jaringan 192.168.1.0/24. Tambahkan akses SSH ke ASA untuk jaringan dalam 192.168.1.0 dengan subnet mask 255.255.255.0 . Tambahkan akses SSH ke ASA dari host 172.16.3.3 di jaringan luar. Pastikan kotak centang **Enable HTTP server for HTTPS/ASDM** dicentang. Klik **Next** untuk melanjutkan.



Gambar 12. Tampilan Startup Wizard

f. Pada layar Startup Wizard Step 12 - Startup Wizard Summary, periksa Configuration Summary dan klik **Finish**. ASDM akan mengirimkan perintah ke perangkat ASA dan kemudian memuat ulang konfigurasi yang dimodifikasi.

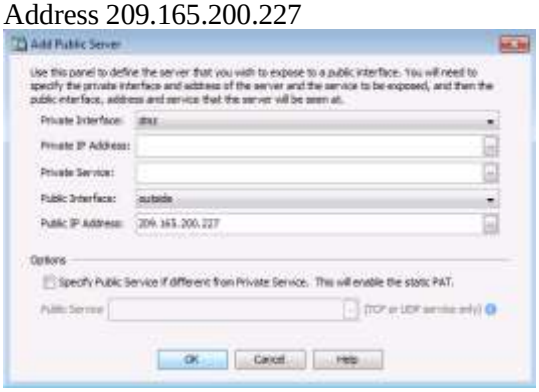
6. Konfigurasi ASA DMZ interface
   Pada **Configuration > Device Setup**, klik **Interface Settings > Interfaces**. Klik dua kali GigabitEthernet1/3 untuk konfigurasi interface dmz. Kemudian isi dialog box Edit Interface sebagai berikut:



Gambar 13. Dialog box Edit Interface

Centang checkbox **Enable traffic between two or more interfaces which are configured with the same security levels** lalu klik **Apply**

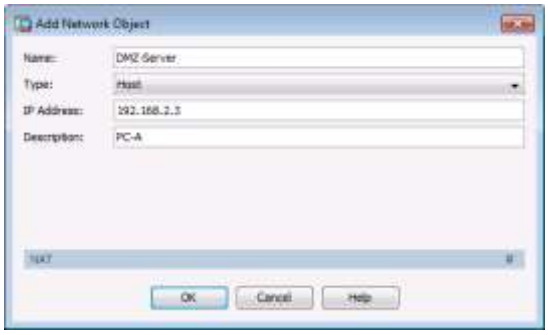
7. Konfigurasi NAT statis ke DMZ
   a. Pada menu **Firewall**, klik opsi **Public Servers** dan klik **Add** untuk menentukan server DMZ dan layanan yang ditawarkan. Di dialog box **Add Public Server**, tentukan Private Interface sebagai dmz, Public Interface sebagai outside, dan Public IP Address 209.165.200.227



Gambar 14. Dialog Add Public Server

   b. Klik tombol yang ada di kanan Private IP Address, maka akan menuju ke dialog box **Browse Private IP Address**. Kemudian klik

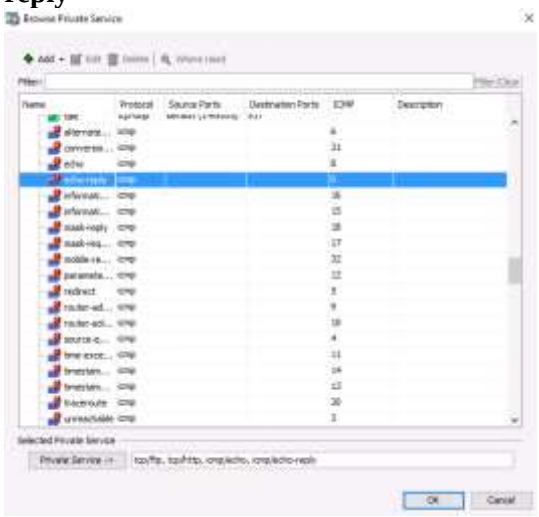
Add untuk menentukan server sebagai Network Object.



Gambar 15. Add Network Object

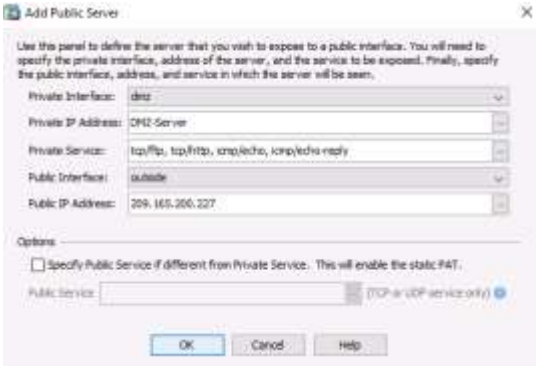
Gambar 16. Browse Private IP Address

c. Kembali ke Add Public Server, klik tombol yang ada di kanan Private Service kemudian pilih servis **tcp/ftp**, **tcp/http**, **icmp/echo**, dan **icmp/echo-reply**



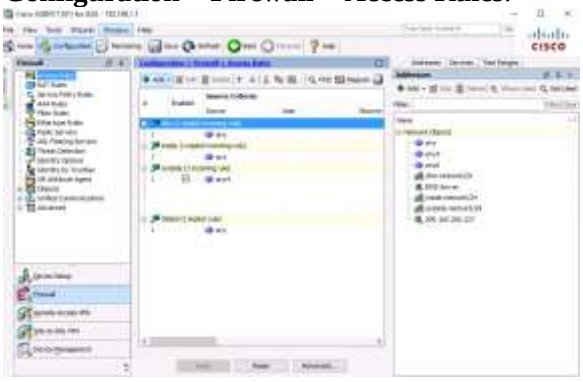
Gambar 15. Browse Private Service

Sehingga isi dari dialog box Add Public Server seperti Gambar 16. Klik **OK** kemudian **Apply**.



Gambar 16. Add Public Server

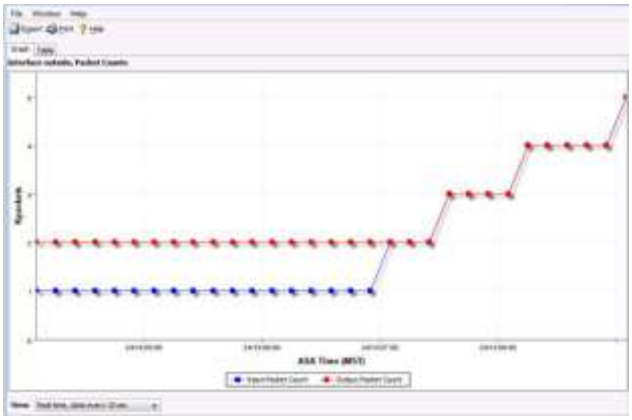
8. Lihat *Access Ruler* (ACL) yang dibuat oleh ASDM.
   Setelah membuat objek server DMZ, ASDM secara otomatis membuat ACL untuk mengizinkan akses yang sesuai ke server dan menerapkannya ke interface outside pada arah yang masuk.
   Melihat ACL pada ASDM dengan memilih **Configuration > Firewall > Access Rules**.



Gambar 17. Access Rules

Perhatikan PC-C, berhasil melakukan ping pada alamat IP dari alamat server public NAT statis. Karena VLAN 1 diatur tingkat keamanan 100 (inside) dan DMZ diatur tingkat keamanan 70, dari host jaringan dalam (PC-B) dapat mengakses server DMZ (PC-A). Hal tersebut dikarenakan tingkat keamanan *interface* dan fakta bahwa ICMP sedang diinspeksi di *inside interface* oleh *global inspection policy*. Namun, server DMZ tidak dapat melakukan ping ke PC-B karena DMZ memiliki tingkat keamanan yang lebih rendah.

Setelah melakukan tes ping berulang dari R2 ke server DMZ dan ping dari PC-B ke R1, menunjukkan grafik di bawah ini. *Input Packet Count* menunjukkan hasil ping dari R2, sedangkan *Output Packet Count* menunjukkan hasil ping dari PC-B.



Gambar 18. Grafik I/O Packet Count

KESIMPULAN

Konfigurasi Firewall ASA menggunakan ASDM dibanding dengan menggunakan CLI lebih mudah dipahami dan diimplementasikan. Pada GUI ASDM, terdapat banyak fitur dan alat yang dapat digunakan untuk mengkonfigurasi firewall ASA, seperti *Device Setup Startup Wizard*, *Public Server*, ACL, dan lain sebagainya. Hasil dari implementasi *Firewall* pada topologi tersebut bahwa jaringan dalam dapat mengakses server DMZ namun DMZ tidak dapat mengakses jaringan dalam, karena DMZ memiliki tingkat keamanan lebih rendah.

DAFTAR PUSTAKA

Kurniawan, Dwi Ely, dkk. (2019). *Implementation and analysis ipsec-vpn on cisco asa firewall using gns3 network simulator*. 1st International Conference on Advance and Scientific Innovation (ICASI).

Trabelsi, Z., & Saleous, H. (2019). Exploring the opportunities of cisco packet tracer for hands-on security courses on firewalls. In *2019 IEEE Global Engineering Education Conference (EDUCON)* (pp. 411-418). IEEE.

Xu, J., & Su, W. (2013). Performance evaluations of Cisco ASA and linux IPTables firewall solutions.

Naik, N., Shang, C., Shen, Q., & Jenkins, P. (2019, June). D-FRI-CiscoFirewall: Dynamic fuzzy rule interpolation for Cisco ASA Firewall. In *2019 IEEE International Conference on Fuzzy Systems (FUZZ-IEEE)* (pp. 1-6). IEEE.

Naik, N., Jenkins, P., Kerby, B., Sloane, J., & Yang, L. (2018, July). Fuzzy logic aided intelligent threat detection in cisco adaptive security appliance 5500 series firewalls. In *2018 IEEE International Conference on Fuzzy Systems (FUZZ-IEEE)* (pp. 1-8). IEEE.

Riyadi, Imam. (2011). *Optimalisasi Keamanan Jaringan Menggunakan Pemfilteran Aplikasi Berbasis Mikrotik*. JUSI Vol 1 No 1. ISSN 2087-8737

Mufadhol, M. (2012). Simulasi Jaringan Komputer Menggunakan Cisco Packet Tracer. *Jurnal Transformatika*, *9*(2), 64-71.

Tarkaa, N. S., Iannah, P. I., & Iber, I. T. (2017). Design and simulation of local area network using cisco packet tracer. *The International Journal of Engineering and Science*, *6*(10), 63-77.

Pratama, I., & Eka, P. A. (2015). Jaringan Komputer. *Informatika*.

Yudianto, M. J. N. (2014). Jaringan Komputer dan Pengertiannya. *Ilmukomputer. Com*, 1-10.

Cisco_A. (n.d.). "Cisco Adaptive Security Appliance (ASA) Software". https://www.cisco.com/c/en/us/products/security/adaptive-security-appliance-asa-software/index.html diakses pada 20 Oktober 2020.

Cisco_B. (n.d). "Cisco Adaptive Security Device Manager". https://www.cisco.com/c/en/us/products/security/adaptive-security-device-manager/index.html diakses pada 20 Oktober 2020.