CESS
(Journal of Computing Engineering, System and Science) 8(1) January 2023 175-183

e-ISSN: 2502-714x
p-ISSN: 2502-7131

Contents list available at www.jurnal.unimed.ac.id

CESS
(Journal of Computing Engineering, System and Science)

journal homepage: https://jurnal.unimed.ac.id/2012/index.php/cess

Implementasi Keamanan Jaringan dan Mengantisipasi *Attacker* Menggunakan *pfSense Firewall*

Implementation of Network Security and Anticipating Attackers Using pfSense Firewall

Alhu Waladan Naufal Sholihan[1*], Aan Restu Mukti[2], Suryayusra[3], Rahmat Novrianda Dasmen[4]

[1,2]Program Studi Teknik Informatika, Universitas Bina Darma
Jalan Raya Jenderal Ahmad Yani No.3,9/10 Ulu, Palembang Sumatera Selatan 30111
email: [1]alhuwaladanns@gmail.com, [2]aanrestu@binadarma.ac.id [3]suryayusra@binadarma.ac.id, [4]rahmatnovrianda@binadarma.ac.id

A B S T R A K

Di PT. PLN (Persero) UPDL Palembang menggunakan router dari cisco seri 1900 series, secara hardware perangkat cisco ini sudah sangat lawas karena dirilis pada tahun 2009 menurut sumber situs cisco, menggunakan cisco seri 1900 series sebagai router merupakan suatu hal yang sangat rentan diserang oleh *attacker* dikarenakan ketertinggalan zaman dalam hal keamanan jaringannya, Dan kurangnya perhatian terhadap keamanan jaringan juga merupakan suatu hal yang menjadi acuan perhatian dalam hal ini, Dengan permasalahan tersebut maka dilakukan penambahan routing untuk keamanan jaringan dengan melakukan perancangan *pc router firewall* dari *pfSense*, *pc router* sendiri menggunakan aset komputer yang sudah tidak terpakai namun memiliki spesifikasi yang cukup, Dengan metode penelitian *action research* melaksanakan diagnosa, merencanakan tindakan, menindak lanjut, mengadakan evaluasi, dan bahan pembelajaran. Dengan merancang *pc router firewall* menggunakan *pfSense* diharapkan akan dapat hasil yang cukup baik, karena menggunakan fitur *firewall* router menggunakan *pfSense* untuk melakukan pemblokiran terhadap penyerangan. Menggunakan *pfSense* ini sebagai keamanan jaringan akan dapat dipastikan lebih aman dikarenakan *pfSense* masih rutin melaksanakan pembaruan atau meningkatkan keamanannya dan memiliki komunitas forum yang aktif sampai saat ini sehingga dapat saling bertukar informasi.

Kata Kunci: *Cisco 1900 Series, pfSense, Firewall, pc router.*

A B S T R A C T

At PT. PLN (Persero) UPDL Palembang uses routers from the Cisco 1900 series, hardware-wise this Cisco device is very old because it was released in 2009 according to a Cisco website source,

**Penulis Korespondensi:*
email: alhuwaladanns@gmail.com

using the Cisco 1900 series as a router is something that is very vulnerable to attack by attackers due to its backwardness. the times in terms of network security, and the lack of attention to network security is also a matter of concern in this regard. With these problems, routing is added for network security by designing a pc router firewall from pfSense, the pc router itself uses computer assets that are is no longer used but has sufficient specifications. Using the action research method, carrying out diagnoses, planning actions, following up, conducting evaluations, and learning materials. By designing a pc router firewall using pfSense it is hoped that the results will be quite good, because it uses the router firewall feature using pfSense to block attacks. Using pfSense as network security will certainly be safer because pfSense still regularly updates or improves its security and has an active forum community to date so that information can be exchanged.

Keywords: *Cisco 1900 Series, pfSense, Firewall, pc router.*

1. PENDAHULUAN

Di PT. PLN (Persero) UPDL Palembang Palembang menggunakan internet dari salah satu ISP yaitu Icon+ yang memiliki *bandwidth* 100MB. Kurangnya perhatian terhadap perangkat jaringan komputer dan keamanan jaringan merupakan hal yang sangat membahayakan karena dapat terkena serangan seperti *DoS* atau *scanning port* yang menyebabkan jaringan down karena membanjiri sistem dengan permintaan yang berlebihan, dikarenakan infrastruktur jaringannya memiliki FTP yang menampung data penting sehingga dapat menyebabkan pencurian data, Namun belum melakukan peningkatan untuk mengamankan jaringan, karena seiring perkembangan jaman keamanan jaringan harus di tingkatkan maka diperlukannya *firewall* yang mumpuni dan lebih baik.

Maka dari itu, dengan permasalahan tersebut kemudian dilakukanlah perancangan *pc router* menggunakan *pfSense*. *Pc router* nya sendiri memiliki spesifikasi ram 8GB tipe ddr4, prosessor yang dipakai intel i3-9100F, dan menggunakan storage 250GB. *pfSense* merupakan sistem operasi yang bersifat *open source* dan berbasis *FreeBSD*, dapat digunakan sebagai *firewall* dan dapat diunduh secara gratis. Daripada itu diperlukanlah perancangan *pc router* sebagai *firewall* menggunakan *pfSense* untuk dapat memberi keamanan jaringan di PT. PLN (Persero) UPDL Palembang dengan fitur IDS (*Intrution Detection System*) dan IPS (*Intrution Prevention System*) yang ada di *pfSense*, Dengan masalah tersebut tujuan dari perancangan ini juga untuk memberi keamanan jaringan sementara atau *prototype* menggunakan *firewall pfSense* dalam meningkatkan keamanan jaringan di PT. PLN (Persero) UPDL Palembang.

2. METODE PENELITIAN

Pada penelitian ini peneliti menggunakan metode yang disebut Tindakan (Action Research).

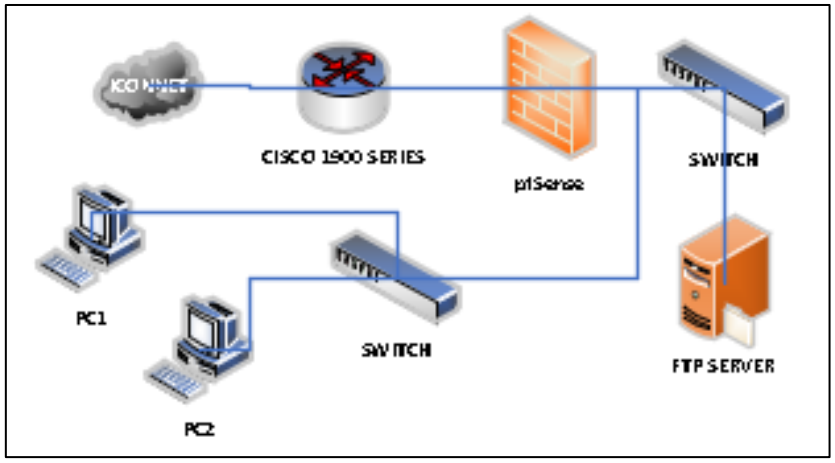
2.1 Melakukan Diagnosa

Pada tahap diagnosa ini penulis mencoba mengidentifikasi suatu permasalahan yang sedang terjadi di jaringan PT. PLN (Persero) UPDL Palembang yang dimana di perusahaan tersebut ini menggunakan satu ISP yaitu icon+ yang memiliki bandwidth 100MB dan menggunakan router dari cisco 1900 series. Yang dimana secara tahun perilisan cisco 1900 series dirilis pada tahun 2009 sementara sekarang sudah memasuki tahun 2023 yang dimana sudah 14 tahun sudah router tersebut dipakai dan secara hardware cisco 1900 series memiliki

spesifikasi yang cukup rendah yaitu hanya memiliki 512GB DRAM dan dari situs cisco itu sendiri seri ini sudah *end of sale* dan tidak mendapat dukungan update lagi dari cisco, karena router cisco yang memiliki keamanan hanya yang mempunyai label firepower, dan router cisco 1900 series juga rawan untuk terkena dos, dengan hal itu ditakutkan akan terjadi pencurian data ataupun jaringan yang down yang dapat disebabkan oleh *attacker.*

2.2 Membuat Rencana Tindakan

Kemudian setelah melakukan diagnosa dan mengidentifikasi suatu masalah yang ditemukan, selanjutnya pada penelitian ini peneliti merencanakan tindakan untuk menyelesaikan indikasi masalah yang dapat ditimbulkan dalam jaringan tersebut. Peneliti menyiapkan sebuah komputer untuk dijadikan sebagai router dan dirouting ke router cisco 1900 series kemudian menyiapkan *port LAN* tambahan untuk ditambahkan ke pc yang akan dijadikan *router/firewall* kemudian diinstall pfsense sebagai keamanan jaringannya. Setelah menyiapkan pc router penulis merancang topologi untuk *pc router firewall pfSense* nya.



Gambar 1. Design Topologi pfSense

Dan pada IP address WAN menggunakan IP address DHCP yang berasal dari ISP kemudian untuk IP address LAN nya sendiri menggunakan IP address static yang berarti kita sendiri yang memasukan IP address dan mengaturnya tidak seperti DHCP. Kemudian dilakukan konfigurasi ke web interface yang alamatnya itu dari IP address WAN dari *pfSense*. Kemudian Langkah selanjutnya setting user dan *password* kemudian DNS serta jaringan LAN disetting DHCP agar client yang terhubung mendapatkan IP address secara otomatis, kemudian peneliti menggunakan fitur IDS (*Intrution Detection System*) dan IPS (*Intrution Prevention System*) yang telah disiapkan oleh *pfSense firewall* untuk mengantisipasi serangan seperti *Denial of Services* (DoS) dan *port scanning*.

3. HASIL DAN PEMBAHASAN

Pada tahap pengujian pertama peneliti menginstall pfSense di komputer yang akan dijadikan router kemudian mengkonfigurasi IP address, setting user dan password kemudian melakukan instalasi IDS (*Intrution Detection System*) dan IPS (*Intrution Prevention System*) yang sudah termasuk didalam *snort* kemudian mengkonfigurasinya di pfSense, kemudian sebelum menghubungkannya peneliti menguji melakukan penyerangan ke router cisco 1900 series dengan melakukan *Denial of Services* (DoS) dan *port scanning ,* Setelah itu peneliti

menghubungkan pc router sesuai dengan design topologi yang sudah dibuat kemudian melakukan penyerangan.

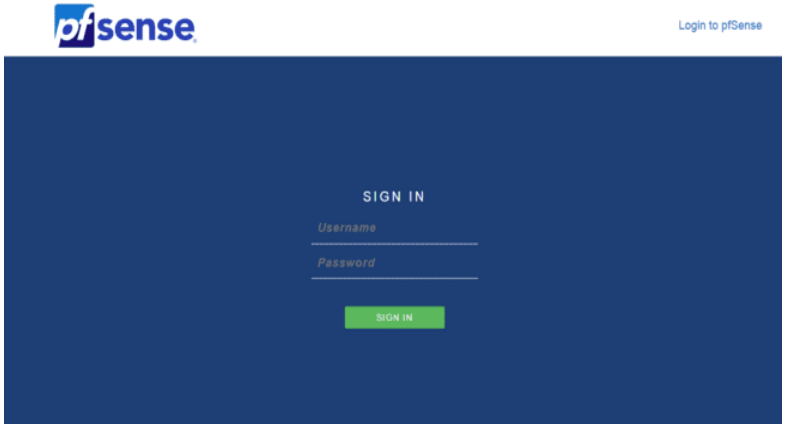
3.1. Konfigurasi pfSense

Pada tahap pertama ini peneliti melakukan konfigurasi IP address WAN untuk dapat mengakses *web interface* dari *pfSense* dan IP address LAN untuk client yang akan terhubung.

Tabel 1. IP Address

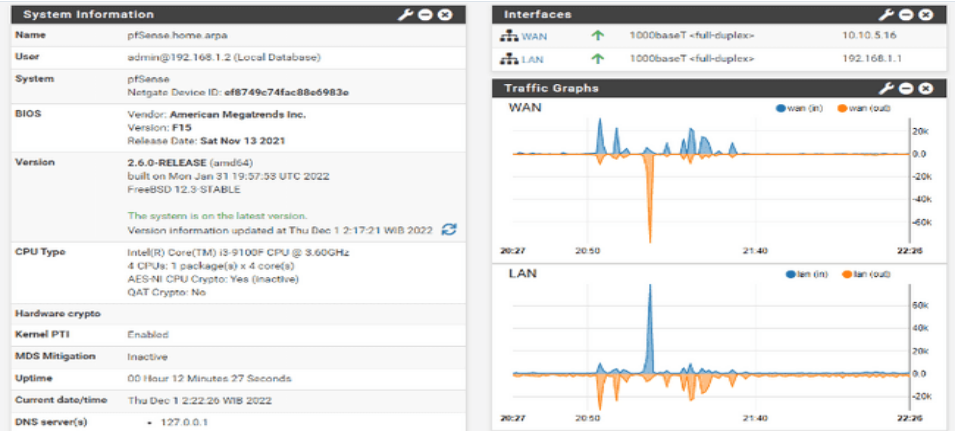
PERANGKAT	IP Address
FTP Server	10.10.5.2
pfSense port WAN (ue0)	192.168.137.119
pfSense port LAN dan Web Interface (alc0)	10.10.5.1
PC 1	10.10.5.3
PC 2	10.10.5.4

Pada gambar 2 menampilkan halaman login, dimana halaman ini adalah pintu agar dapat masuk kedalam dashboard pfSense, untuk default passwordnya sendiri adalah user : admin password : pfsense.



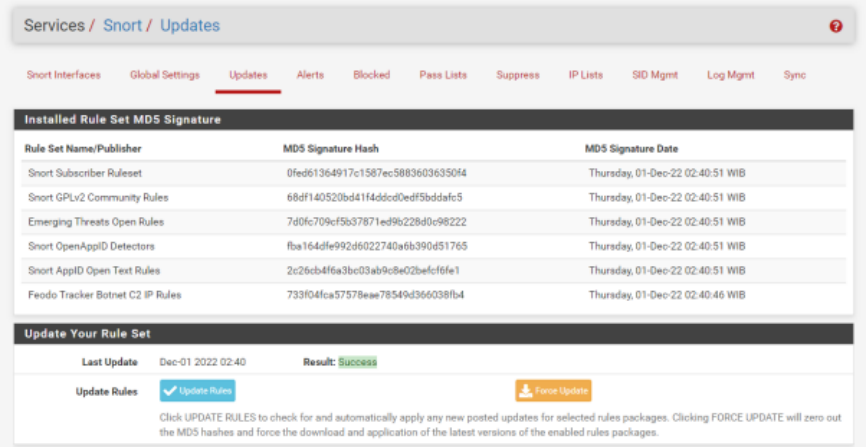
Gambar 2. Tampilan Menu Login

Pada gambar 3 menampilkan halaman antarmuka setelah melakukan proses login, disini pfsense menampilkan System Information, Interfaces, dan Traffic Graphs.



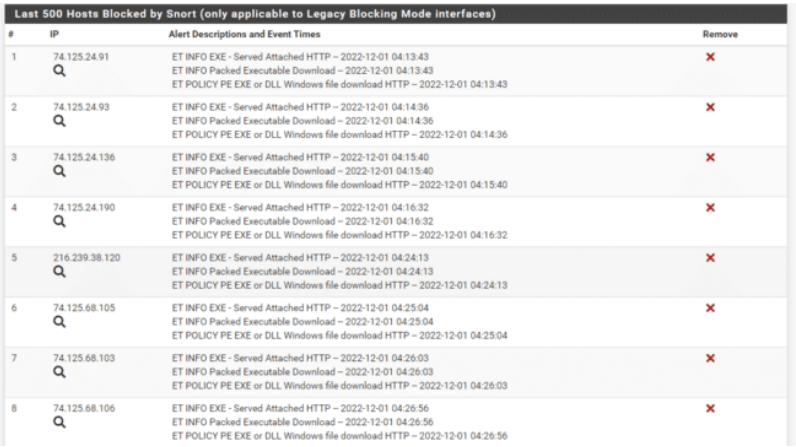
Gambar 3. Tampilan Awal

Tampilan pada gambar 4 merupakan update rules snort agar snort dapat mendeteksi serangan yang terjadi.



Gambar 4. Pengaturan Snort

Berikut adalah percobaan scanning dilakukan di sistem operasi windows ke ip FTP Server menggunakan nmap untuk mengetahui port apa saja yang terbuka.bKetika masuk ke menu alert di interface WAN terdeteksi sedang terjadi proses mencurigakan terdapat 21 Entries in Active Log.



Gambar 5. Blocked by Snort

Kemudian pada menu Blocked terlihat snort melakukan proses block, Hosts Blocked by Snort (only applicable to legacy blocking mode interfaces). Dilakukan percobaan lagi untuk melakukan scanning dan hasilnya tidak bisa mendapatkan informasi port yang terbuka lagi.

Agar snort dapat mendeteksi serangan DDOS perlu dilakukan custom rules di snort, Masukkan code custom rules untuk snort dapat mendeteksi serangan ddos attack detection atau ping of death detection.

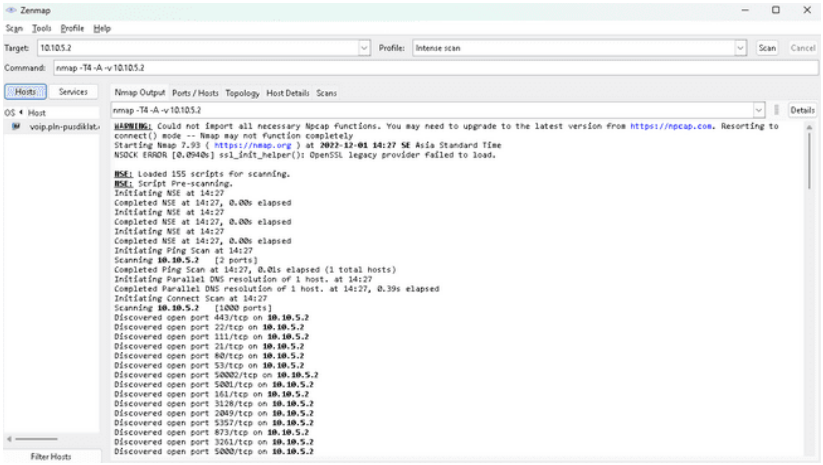
3.2. Percobaan Penyerangan Sebelum Menggunakan Pfsense

Pada tahap kedua ini peneliti melakukan percobaan penyerangan ke FTP Server sebelum menggunakan *pfSense*, percobaan penyerangan menggunakan metode *Denial of Services* (DoS) dan *port scanning,* penyerangan DoS menggunakan low orbit ion cannon ditargetkan ke IP address FTP Server terlihat pada Gambar dan *port scanning* menggunakan nmap pada Gambar.

Ketika mencoba mencoba test ping ke IP address FTP Server hasil respon nya *request timed out* kemudian hasil dari scanning port terbaca beberapa port yang terbuka.

Gambar 6. Low Orbit Ion Cannon

Berikut adalah percobaan scanning dilakukan di sistem operasi windows ke ip FTP Server menggunakan nmap untuk mengetahui port apa saja yang terbuka.



Gambar 7. Scanning Port Nmap

Dari hasil scan didapat port yang terbuka yang ditunjukkan pada tabel 2.

Tabel 2. Open Port

Keterangan	Open Port
Discovered open port	433/tcp on 10.10.5.2
Discovered open port	22/tcp on 10.10.5.2
Discovered open port	111/tcp on 10.10.5.2
Discovered open port	21/tcp on 10.10.5.2
Discovered open port	80/tcp on 10.10.5.2
Discovered open port	53/tcp on 10.10.5.2
Discovered open port	50002/tcp on 10.10.5.2
Discovered open port	5001/tcp on 10.10.5.2
Discovered open port	161/tcp on 10.10.5.2
Discovered open port	3128/tcp on 10.10.5.2

Hasil dari pengujian sebelum menghubungkan pfSense dan melakukan serangan dampaknya dapat menyebabkan FTP Server mengalami down sementara ketika dilakukan serangan *Denial of Services* (DoS) dan pada saat dilakukan port scanning informasi port yang terbuka sangat banyak sekali informasi yang bisa didapat sehingga ini sangat membahayakan bagi jaringan yang diserang serta data-data yang kemungkinan dapat dicuri atau disalahgunakan, Hal ini disebabkan router cisco 1900 series belum memiliki sistem keamanan seperti firewall atau apapun yang dapat memblok aktivitas mencurigakan.

3.3. Percobaan Penyerangan Sesudah Menggunakan Pfsense

Pada tahap ketiga ini sebelum melakukan percobaan penyerangan peneliti menggunakan fitur IDS (*Intrution Detection System*) dan IPS (*Intrution Prevention System*) yang tersedia di pfSense firewall, kemudian peneliti mencoba kembali melakukan penyerangan dengan metode *Denial of Services* (DoS) dan *port scanning* ke FTP Server dengan kondisi jaringan sudah memiliki keamanan jaringan menggunakan firewall pfSense.

Tabel 3. Hasil Pengujian Port Scanning di pfSense.

Date/Time	Protokol	Class	Source IP	Destination IP	Description
2022-12-01 04:26:03	TCP	Potential Corporate Privacy Violation	74.125.68.103	10.10.5.2	ET POLICY PE EXE or DLL Windows file download HTTP
2022-12-01 04:26:03	TCP	Misc activity	74.125.68.103	10.10.5.2	ET INFO Packed Executable
2022-12-01 04:26:03	TCP	Misc activity	74.125.68.103	10.10.5.2	ET INFO EXE - Served Attached HTTP
2022-12-01 04:26:04	TCP	Potential Corporate Privacy Violation	74.125.68.103	10.10.5.2	ET POLICY PE EXE or DLL Windows file download HTTP
2022-12-01 04:26:04	TCP	Misc activity	74.125.68.103	10.10.5.2	ET INFO Packed Executable Download
2022-12-01 04:26:04	TCP	Misc activity	74.125.68.103	10.10.5.2	ET INFO EXE - Served Attached HTTP

Tabel 4 menunjukkan hasil *blocked port scanning* menggunakan pfsense

Tabel 4. Blocked Port Scanning di pfSense.

IP	Alert Descriptions and Event Times
74.125.24.91	ET INFO EXE - Serverd Attached HTTP - 2022-12-01 04:13:43 ET INFO Packed Executable Download - 2022-12-01 04:13:43 ET POLICY PE EXE or DLL Windows file download HTTP - 2022-12-01 04:13:43
74.125.24.93	ET INFO EXE - Serverd Attached HTTP - 2022-12-01 04:14:36 ET INFO Packed Executable Download - 2022-12-01 04:14:36 ET POLICY PE EXE or DLL Windows file download HTTP - 2022-12-01 04:14:36

74.125.24.136	ET INFO EXE - Serverd Attached HTTP - 2022-12-01 04:15:40 ET INFO Packed Executable Download - 2022-12-01 04:15:40 ET POLICY PE EXE or DLL Windows file download HTTP - 2022-12-01 04:15:40
74.125.24.190	ET INFO EXE - Serverd Attached HTTP - 2022-12-01 04:16:32 ET INFO Packed Executable Download - 2022-12-01 04:16:32 ET POLICY PE EXE or DLL Windows file download HTTP - 2022-12-01 04:16:32
74.125.24.120	ET INFO EXE - Serverd Attached HTTP - 2022-12-01 04:24:13 ET INFO Packed Executable Download - 2022-12-01 04:24:13 ET POLICY PE EXE or DLL Windows file download HTTP - 2022-12-01 04:24:13
74.125.24.105	ET INFO EXE - Serverd Attached HTTP - 2022-12-01 04:25:04 ET INFO Packed Executable Download - 2022-12-01 04:25:04 ET POLICY PE EXE or DLL Windows file download HTTP - 2022-12-01 04:25:04

Hasil pengujian DDoS menggunakan pfSense ditunjukkan pada tabel 5.

Tabel 5. Hasil Pengujian DDoS di pfSense

Date/Time	Protokol	Class	Source IP	Destination IP	Description
2022-12-06 01:50:53	TCP	Misc activity	10.10.5.3	13.107.4.52	ET INFO Microsoft Connection Test
2022-12-06 01:50:53	TCP	Misc activity	10.10.5.3	13.107.4.52	ET INFO Microsoft Connection Test
2022-12-06 01:50:53	TCP	Misc activity	10.10.5.3	13.107.4.52	ET INFO Microsoft Connection Test
2022-12-06 01:50:53	TCP	Misc activity	10.10.5.3	13.107.4.52	ET INFO Microsoft Connection Test

Hasil *blocked* DDoS menggunakan pfSense ditunjukkan pada tabel 6.

Tabel 6. Blocked DDoS di pfSense

IP	Alert Descriptions and Event Times
74.125.24.136	Possible UDP DoS - 2022-12-06 01:46:03
74.125.20.204	Possible UDP DoS - 2022-12-06 01:46:40
66.96.226.205	Possible UDP DoS - 2022-12-06 01:46:45
142.251.91.138	Possible UDP DoS - 2022-12-06 01:47:37

Hasil dari pengujian sesudah menghubungkan pfSense dan melakukan serangan dampaknya cukup menjaga FTP Server dari serangan seperti *Denial of Services* (DoS) dan port scanning dikarenakan pfSense mempunyai fitur IDS (*Intrution Detection System*) dan IPS (*Intrution Prevention System*) sehingga ketika penyerangan sedang berlangsung maka ada notifikasi alert yang memberitahukan bahwa ada penyerangan dan disertakan Source IP

penyerang kemudian otomatis pfSense akan memblokir aktifitas mencurigakan tersebut sehingga penyerang tidak dapat menyerang kembali.

4. KESIMPULAN

Berdasarkan penelitian yang telah dilakukan router cisco 1900 series tidak bisa melindungi FTP Server dari serangan DDoS dan port scanning, bahkan dapat membuat FTP Server tidak bisa diakses ketika terkena DDoS maka hal ini sangatlah berbahaya karena tidak adanya keamanan jaringan di PT. PLN (Persero) UPDL Palembang dan dapat menimbulkan pencurian data sedangkan *pc router firewall pfSense* berhasil diterapkan sebagai keamanan jaringan sementara untuk mencegah adanya serangan DDoS dan *port scanning*. Dengan menggunakan *snort* yang didalamnya mempunyai fitur IDS (*Intrution Detection System*) dan IPS (*Intrution Prevention System*), dari proses percobaan *pfSense* cukup responsif dalam merespon serangan/aktifitas mencurigakan dan langsung melakukan pemblokiran terhadap *source IP* yang melakukan penyerangan.

REFERENSI

[1] Hafiz. (2020). Pengertian, Contoh Dan Cara Kerja Intrusion Prevention System (IPS). Diakses 11 September 2022: https://aliyhafiz.com/pengertian-contoh-klasifikasi-cara-kerja-intrusion-prevention-system-ips/
[2] Setiawan, Rony. (2021). Mengenal Apa Itu Firewall dengan Lebih Baik. Diakses 11 September 2022: https://www.dicoding.com/blog/apa-itu-firewall/
[3] Immersa. (2018). Pengertian Ids Security, Jenis, Dan Cara Kerjanya. Diakses 11 September 2022: https://www.immersa-lab.com/pengertian-ids-jenis-dan-cara-kerjanya.htm
[4] Rajendra, Laksamana. (2022). Proxy Server. Diakses 11 September 2022: http://sistem-informasi-s1.stekom.ac.id/informasi/baca/Proxy-Server/91ea14e6f9df9b906f4d309a31215ca76876bf6c
[5] Zientara, David. (2018). Mastering pfSense. Birmingham: Packt Publishing Ltd.
[6] Rafiudin, Rahmat. (2010). Mengganyang Hacker Dengan Snort. Yogyakarta: Andi.
[7] Napizahni, Mike. (2022). DDoS Attack: Pengertian, Jenis, dan Cara Mencegahnya. Diakses 30 Januari 2023: https://www.dewaweb.com/blog/ddos-attack-pengertian-dan-solusinya/
[8] Fauzan, Muhammad Afif Al dan Timur Dali Purwanto. (2021). Perancangan Firewall Router Menggunakan Opnsense Untuk Meningkatkan Keamanan Jaringan PT. Pertamina Asset 2 Prabumulih," Seminar Hasil Penelitian Vokasi (SEMHAVOK). Universitas Bina Darma, ISSN: 2654-5438
[9] Valianta, Sasut Analar, Tasmi, Deris Stiawan," Identifikasi Serangan Port Scanning dengan Metode String Matching," Jurnal ANNUAL RESEARCH SEMINAR 2016, vol. 2, no. 1, pp. 466-471, 2016