Jurnal Pekommas Vol. 10 No. 1, Juni 2025: 29 – 38

Analisis dan Mitigasi Kerentanan DDoS pada Infrastuktur Jaringan dengan Teknik *Hierarchical Clustering* dan *Firewall IPTables*

Analysis and Mitigation of DDoS Vulnerabilities in Network Infrastructure using Hierarchical Clustering and IPTables Firewall Techniques

Hillman Akhyar Damanik[1)], Merry Anggraeni[2)]

Fakultas Teknologi Informasi Universitas Budi Luhur

Jl. Ciledug Raya, Petukangan Utara, Jakarta Selatan, DKI Jakarta, Indonesia 1226012
hillmanakhyardamanik@gmail.com

Diterima: 22 Maret 2024 || Direvisi: 10 November 2024 || Disetujui: 15 Maret 2025

Abstrak – Keamanan infrastruktur jaringan termasuk perangkat router dan server, yang terhubung langsung ke global internet telah menjadi masalah penting seiring dengan meningkatnya komunikasi internet dalam menjaga kerahasiaan, integritas dan ketersediaan komunikasi digital. Masalah paling krusial merupakan infrastruktur jaringan untuk monokultur perangkat router dan server yang diekspolitasi dan mendeteksi serangan *Distributed Denial-of-Service* (DDoS). Penelitian ini bertujuan menggabungkan teknik analisis dan mitigasi dengan *Hierarchical Clustering single linka*ge, *complete link*age, *average linkage* dan *ward linkage* serta tindakan mitigasi *filtering* firewall IPTables, untuk menganalisis data *logging* DDoS pada suricata NIDS, dengan *severity level low, medium* dan *high* yang dieksploitasi dari jaringan *public*. Pengelompokan penyebaran *single linkage* menghasilkan cluster 3 dengan tingkat intensitas *logging* DDoS dengan *severity high*, pada tipe protocol TCP *Sync Flood*. Cluster 3 menghasilkan *severity high* source IP *address*. Clustering *complete linkage* menghasilkan potensi *high logging* DDoS, terdapat pada cluster 1 dan cluster 2. Hasil penyebaran *average linkage* menunjukkan kelompok dengan *severity* level *average low* untuk DDoS. Teknik *Ward linkage* menghasilkan kelompok yang lebih seragam pada atribut pada setiap *n_clusters* 1 sampai cluster 6. Implementasi teknik mitigasi dengan IPSet dan firewall *scripting* IP Tables memberikan hasil positif dalam mengurangi beban kerja perangkat router dan vServer saat menghadapi serangan DDoS. Setelah konvergensi status running menghasilkan beban kerja dari sumber daya vCPU mengalami penuruan persentasi vCPU vR1 10%, vCPU vR2 9% dan memory 11%.
Kata Kunci: Hierarchical Clustering, DDoS, IPTables, Suricata NIDS

Abstract *– Network Security infrastructure including routers and server devices, which are connected directly to the global internet has become an important issue along with the increase in internet communications in maintaining the confidentiality, integrity and availability of digital communications. The most challenging problem is the network infrastructure for exploiting a monoculture of routers and servers and detecting Distributed Denial-of-Service (DDoS) attacks. This research aims to combine analysis and mitigation techniques with Hierarchical Clustering single linkage, complete linkage, average linkage and ward linkage as well as IPTables firewall filtering mitigation measures, to analyze DDoS logging data on NIDS suricata, with low, medium and high severity levels exploited from the network public. Clusteirng single linkage deployments produces cluster 3 with a DDoS logging intensity level of high severity, on the TCP Sync Flood protocol type. Cluster 3 shows high severity for the source IP address. The complete linkage clustering technique also provides significant results with a large number of potential DDoS logging, found in cluster 1 and cluster 2. The results of the average linkage distribution show a group with a low average severity level for DDoS. The Ward linkage clustering produces a more uniform group of attributes for each n_clusters 1 to cluster 6. Implementation of mitigation techniques with IPSet and firewall scripting IP Tables provides positive results in reducing the workload of router and vServer devices when facing DDoS attacks. After convergence, the running status resulted in the workload of vCPU resources experiencing a decrease in the percentage of vCPU vR1 by 10%, vCPU vR2 by 9% and memory by 11%.*

Keywords: *Hierarchical Clustering, DDoS, IPTables, Suricata NIDS*

PENDAHULUAN

Implementasi perlindungan infrastruktur jaringan dari serangan *cybercriminal* sangat penting untuk menjaga keamanan dan kelangsungan operasi bisnis perusahaan. Internet dan komunikasi digital saat ini menghubungkan miliaran perangkat fisik berupa

doi: 10.56873/jpkm.v9i1.5551

router dan server (Damanik et al., 2023). Perangkat router dan server, yang terhubung langsung ke global internet sering kali tidak aman dan memiliki kerentanan yang berbeda, yang disebabkan oleh pertumbuhan informasi dan jaringan yang berkembang pesat (Damanik, 2022) (Damanik & Anggraeni, 2018) (Huang et al., 2019) (Yamamoto & Yamaguchi, 2023). Penelitian sebelumnya terkait permasalahan pada infrastruktur jaringan terutama pada perangkat server dan router, menuntut ketahanan jaringan terutama dari *cybercriminals*, sehingga harus meningkatkan standar yang harus ditangani oleh sistem keamanan yang lengkap (Adedeji et al., 2023) (Abdullayeva, 2022) (May & Koay, 2019). Penyusupan anomali serangan pada skala jaringan, perlu adanya pemantauan berupa *rule* dan firewall *filtering* untuk menyelidiki operasi serangan dan penyusupan yang dilakukan melalui akses yang tidak sah (Patel, 2020) (Gupta, 2018). Penelitian sebelumnya serangan DDoS menggunakan komputer fisik. Berdasarkan pengujian secara keseluruhan diperoleh hasil penggunaan CPU IDS Snort stabil di angka 55%-58%. Sedangkan hasil berbeda diperoleh *intrusion detection system* (IDS) Suricata, dimana penggunaan CPU lebih baik dibandingkan IDS Snort 10% - 40% (Faiz et al., 2022). Penelitian dengan strategi hibrid menggabungkan Suricata, sebuah sistem deteksi intrusi (IDS), dengan firewall pfSense, untuk mengatasi serangan DdoS (Praptodiyono et al., 2023). Namun pada penelitian tersebut tidak dilakukan dengan mengintegrasikan algortima *clustering*, sehingga belum menghasilkan akurasi pendeteksian yang lebih baik berdasarkan hasil dari pengelompokan. Adapun penelitian IDS dengan algoritma *clustering* telah banyak diterapkan, diantaranya, teknik K-Means digunakan membangun model perilaku serangan, dengan mengekstrak fitur dari sesi serangan dan hasil numerik menunjukkan bahwa metode yang diterapkan dapat mendeteksi secara efektif (She et al., 2016). K-Means juga digunakan menentukan pola serangan DoS pada dataset ISCX membentuk pola dimana sebagian besar IP host-nya hanya dieksploitasi ke satu server (Putri et al., 2017). Dalam penelitian (Jasim & Gaata, 2022), algoritma clustering K-Means diterapkan untuk klasifikasi DDoS, dengan melatih dan menguji dataset CICIDS2017, dengan 2 *centroid* optimal dan normal. Berbeda dengan penelitian *logging* honeypot pada perangkat server dan router dari public internet, teknik K-Means menghasilkan jumlah kuadrat jarak *cluster* ke pusat *cluster* terdekat, ditimbang dengan bobot nilai μi dan persentase jumlah serangan sebesar 64% untuk kategori *high*, 36% *medium* dan *low* dengan jumlah tahapan *clustering* sebanyak 3 tahapan iterasi *cluster* yang sesuai. Mitigasi menghasilkan histori beban kerja CPU berkurang menjadi 28%, dan memory 39%. vFarm Server menunjukkan beban kerja CPU pada masing-masing vServer berkurang menjadi 43% dan Memory (RAM) menjadi menjadi 21% (Damanik & Anggraeni, 2024).

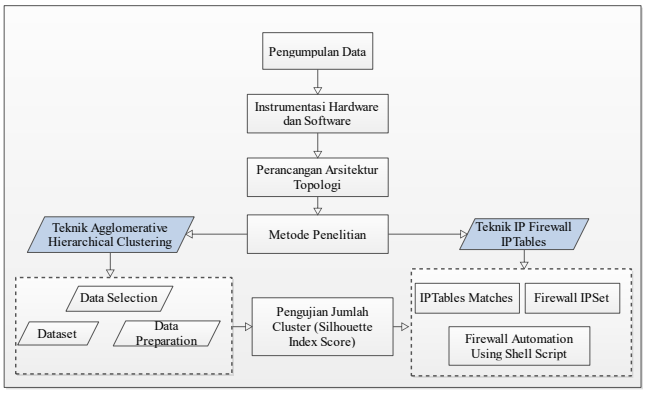
Studi dan penelitian dengan algoritma *supervised learning* juga telah banyak dilakukan dengan sistem IDS, diantaranya penelitian menggunakan *dataset* CICDDoS2019. Hasil dari penggunaan algoritma *supervised* menunjukkan model *Machine Learning* (ML) cukup berhasil mendeteksi lalu lintas serangan DDoS. Penelitian memberikan kontribusi dalam eksperimen, metode pemilihan fitur *random forest regressor* (RFR) meningkatkan akurasi metode ML dalam mendeteksi lalu lintas serangan (Alzahrani & Alzahrani, 2021). Teknik ML seperti k-means, K-*Nearest Neighbors* (KNN), dan Naive Bayes (NB) juga digunakan dalam sistem deteksi intrusi (IDS). Hasil tinjauan menyoroti faktor evaluasi keakuratan jaringan berkecepatan tinggi, memberikan taksonomi serangan DDoS terperinci, dan mengklasifikasikan teknik deteksi (Haseeb-ur-rehman et al., 2023). Kemudian algoritma *Support Vector Machine* (SVM) dan logika Fuzzy dari *log* suricata, juga menghasilkan akurasi pendeteksian yang lebih baik, dengan FPR (*false positif rate*) sebesar 8,6% dan FNR (*false negative rate*) sebesar 2,2% (Shah & Issac, 2018). Namun dari beberapa penelitian tersebut tidak memfokuskan dan mengintegrasikan dengan teknik mitigasi, dari hasil pengelompokan dan klasifikasi hasil serangan dan *logging* DDoS.

Dalam kebaruan penelitian ini, sistem suricata NIDS akan diterapkan di lingkungan virtual network infrastruktur, terletak pada *upstream gateway* dan dialokasikan *bridge interface* dengan perangkat hypervisor proxmox yang terdapat node vServer dan router. Monitoring dan analisis serangan berupa kategori *Source* IP *Address*, *Destination* IP *Address*, *Source Port*, *Destination Port*, *Packet Length* dan *Anomaly Score* dengan *clustering* tiga level serangan (*severity level*) *low*, *medium*, dan *high*, dan pengujian *single linkage, complete linkage, average linkage* dan *ward linkage* Agglomerative Hierarchical Clustering (AHC) dengan *Silhouette Index Score* antara 6 cluster sebagai pengelompokan dataset. Metode rule *filtering*

IPTables digunakan untuk teknik mitigasi dalam percobaan serangan dari hasil pengelompokan, dan teknik mitigasi menguji perbandingan beban kerja CPU dan Memory (RAM) sebelum dan sesudah operasional eksperimen dilakukan.

METODOLOGI PENELITIAN

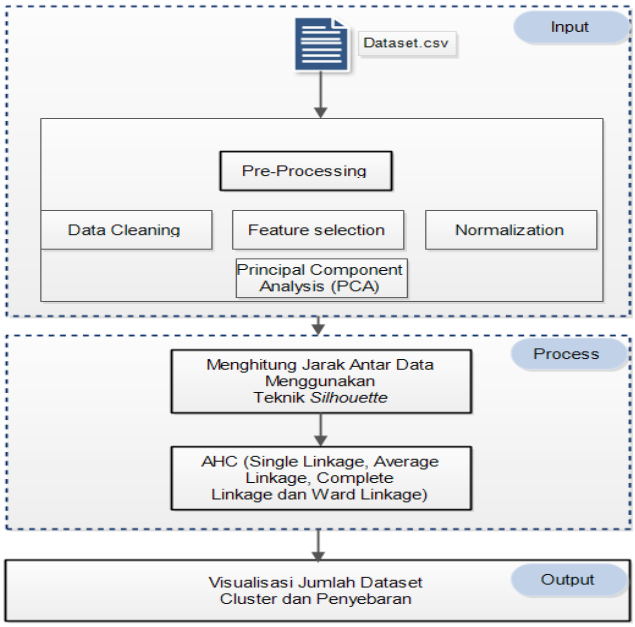
Dalam penelitian ini, penulis menerapkan metodologi terperinci dengan konsep yang dilakukan dalam penelitian dengan mempelajari teori-teori, metode dan konsep pada *trend* dan mekanisme dari struktur yang dimodelkan. Meliputi beberapa prosedur penerapan dan secara garis besar melalui beberapa tahapan seperti pada *flowchart* Gambar 1.



Gambar 1 Metode dan Tahapan Penelitian

Penerapan Teknik Agglomerative Hierarchical Clustering

Selama percobaan, arsitektur suricata melakukan pendekatan untuk mendapatkan file *logging* DDoS pada log server dan router unutk hasil dari *fast.log* dan *eve log format* dan secara bersamaan memproses data *input*, *process* dan *output*. Adapun arsitektur umum implementasi algoritma *Hierarchical Clustering* pada Suricata NIDS pada infrastruktur jaringan ini dapat dilihat pada Gambar 2.



Gambar 2 Implementasi *Hierarchical Clustering* pada Log Dataset Suricata NIDS

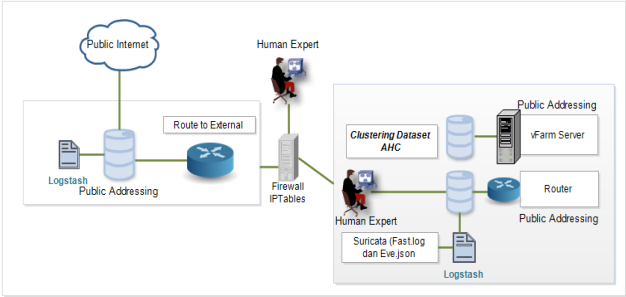
Pre-processing Dataset

Tahap *pre-processing dataset* dalam proses data *cleaning, feature selection, principal component analysis* (PCA) dan *normalization* dataset log suricata yang sebelumnya dikonversi dan diekstrak menjadi ekstensi csv (Vanin et al., 2022). Persiapan data pada dataset penelitian ini akan memilih *field* yang diperlukan sebagai fitur untuk melatih model menggunakan teknik *single linkage, complete linkage, average linkage* dan *ward linkage* AHC. Data *cleaning* dilakukan dengan menghapus dataset pada setiap *attribute* yang memiliki nilai *null* atau mengisi nilai *null* pada setiap *attribute* dataset dengan nilai *mean* kolom tersebut. Pengelompokan dataset dari log suricata digunakan adalah *source addressing, destination addressing, source port, destination port, packet length dan anomaly score, attack type* dan *severity level*, dengan melakukan *handling missing* data dan *Feature Scaling*.

Arsitektur Penerapan Firewall IPTables

Penerapan *rule* Firewall IPTables diimplementasikan seperti topologi pada Gambar 3. *Rule* Firewall *policy* yang dikombinasikan dengan konektivitas suricata NIDS untuk *rule* yang diberikan pada kernel untuk mengatur setiap paket *incoming* dan *outgoing* dalam melakukan *rule filtering* menuju perangkat *gateway*, vFarm Server dan Router yang melewati Router eksternal. *Policy rule* ini akan diterapkan berdasarkan koneksi HTTP *Flood, ICMP Flood,* dan TCP Sync Flood. Firewall IPTables pada

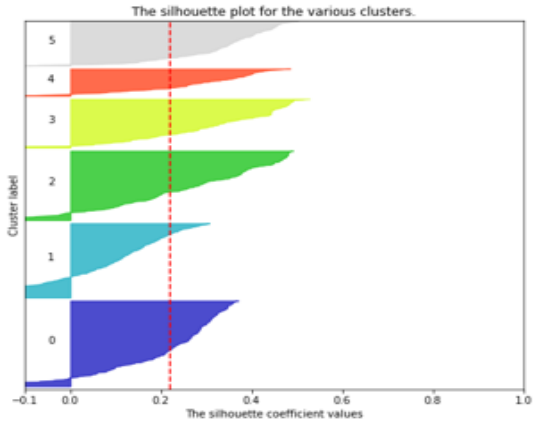
eksperimen ini juga digunakan untuk menyediakan metode meminimalisir *load* pada perangkat vFarm Server dan vRouter, baik penggunaan CPU dan Memory (RAM).



Gambar 3 Penerapan Firewall IPTables

Pengujian Jumlah Cluster dengan Silhouette Index Score

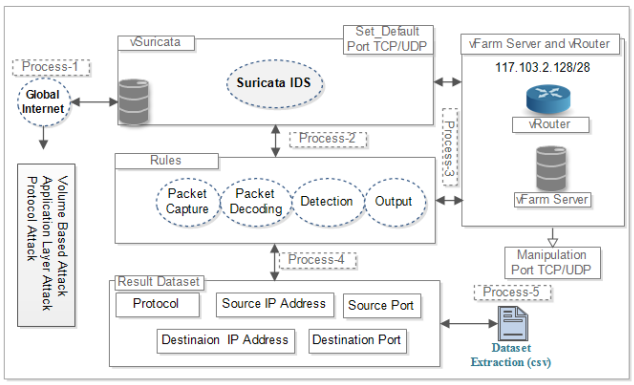
Silhouette score digunakan untuk mengevaluasi kualitas pengelompokan dalam kumpulan dataset dari *logging* DDoS Suricata dengan sintaks `AgglomerativeClustering(n_clusters=n_clusters,affinity='euclidean', linkage='single, complete, average or ward')`. Dari hasil evaluasi dengan *Silhouette* jumlah klaster yang ditentukan adalah *n_cluster* = 6 (*k*=6) (Shutaywi & Kachouie, 2021). Pemilihan cluster dengan memberikan nilai *Silhouette score* tertinggi dari evaluasi banyaknya jumlah cluster yang dilakukan dari 2-10 *cluster*, yaitu dari hasil *cluster n_clusters* = 6, *average silhouette_score* yang dihasilkan adalah dengan nilai 0.219 seperti pada Gambar 4.



Gambar 4 Grafik *k-Cluster Silhouette Index*

HASIL DAN PEMBAHASAN

Eksperimen dilakukan antara 19 November 2023 pukul 17:00 dan 20 Desember 2023 pukul 23:59, dan terdapat 1758 entri *row log* suricata untuk *entry source addressing, destination addressing, source port, packet length dan anomaly score, attack type dan severity level*, yang mendominasi pada protocol TCP/UDP, dari hasil log entry service *suricata.yaml* yang berbeda dihasilkan. Sistem suricata IDS yang didesain mengikuti kerangka kerja *packet capture*, *packet decoding*, *detection* dan *output* yang meniru service yang dapat dieksploitasi dari global internet seperti pada Gambar 5. Kerangka kerja suricata NIDS mengumpulkan semua log dari setiap suricata.yaml dan memusatkannya dari semua serangan terhadap setiap layanan.

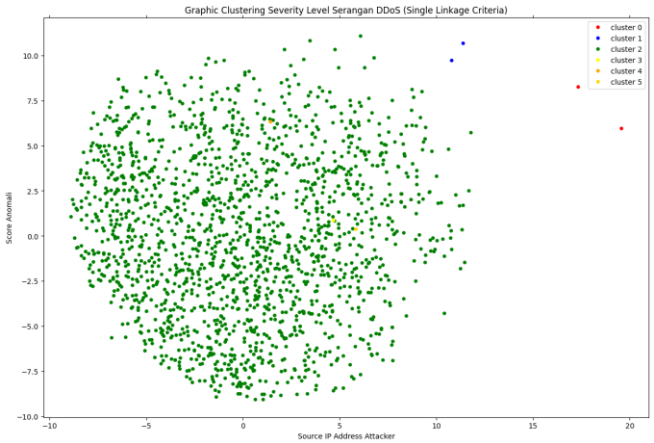


Gambar 5 Kerangka Kerja Suricata NIDS

Konfigurasi pada topologi akan menempatkan suricata pada *gateway* yang terhubung langsung dengan internet, agar koneksi yang ditangkap oleh log *rule* suricata dan merupakan koneksi trafik murni dari luar tanpa adanya *filter* dari *gateway*. Terdapat dua *virtual* server dan 1 vRouter yang menggunakan IP Address public menggunakan skema *bridge management*, dibandingkan dengan gambaran terstruktur dan komprehensif tentang penelitian tentang deteksi anomali dari host komputer (Jose et al., 2018).

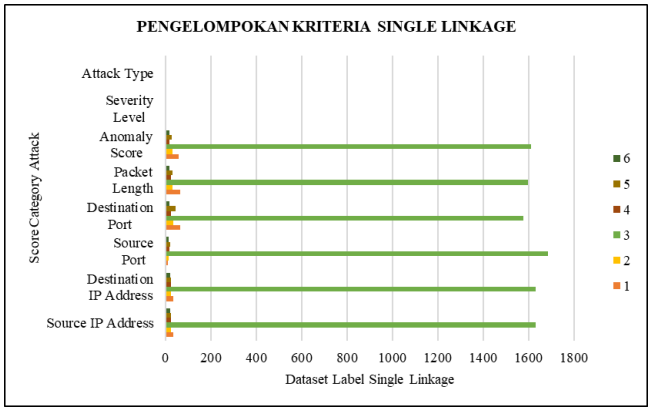
Pengelompokan *Single Linkage* Berdasarkan Kategori Serangan

Penerapan hasil pengujian yang dilakukan dengan metode *single linkage*, bertujuan untuk mengetahui hasil deteksi dan anomali dari *policy* dan *rules* yang dikonfigurasi pada *suricata.yaml* untuk perangkat vServer dan router. Pengukuran jarak dilakukan dengan kelompok dari atribut dataset berdasarkan jarak terdekat. Hasil dari Pengujian yang digunakan adalah *logging* DDoS yang dihasilkan dari public internet dengan hasil monitoring berupa protocol TCP/UDP/ICMP. Jenis DDoS yang digunakan dan dimonitoring adalah tipe serangan TCP *Syn Flood*, ICMP *Flood* dan HTTP *Flood*. Dataset dikelompokkan menjadi 6 cluster yaitu C1, C2, C3, C4, C5, dan C6.



Gambar 6 Grafik Penyebaran Kategori Serangan Kriteria *Single Linkage* Serangan

Penyebaran cluster C1, C2, C3, C4, C5 dan C6 dari clustering dataset, ditampilkan pada Gambar 6. Dimana sebaran titik berwarna *purple* (cluster 1) menampilkan dengan kriteria *single linkage*, dengan kondisi jenis serangan kategori tipe TCP *Sync Flood* dari 35 *source* IP *address* cluster 1 dan *destination* IP *address* sebanyak 35, 10 *source* port, 65 *destination* port, 65 *packet length* dan 56 *anomaly score*. Cluster 1 menghasilkan jumlah *source* IP *address* dengan potensi *low* dari lalu lintas serangan (*logging* DDoS) tipe protocol TCP *Sync Flood*. Sebaran titik berwarna *blue* pada cluster 2 sebanyak 24 *source* IP *address* dan 24 *destination address*, 13 *source* port, 35 *destination* port, 30 *packet length*, 30 *anomaly score* dengan kategori *severity level high*. Cluster 2 menghasilkan jumlah *source* IP *address* dengan potensi *low* dari lalu lintas serangan (*logging* DDoS) tipe protocol TCP *Sync Flood*. Cluster 3 membentuk sebaran titik berwarna *green* dengan 1630 *source* IP *address*, 1630 *destination* IP *address*, 1685 *source* port, 1575 *destination* port, 1595 *packet length*, dan 1610 *anomaly score* dengan kategori medium dengan tipe serangan ICMP *Flood* dengan *severity level high*. Cluster 4 dengan sebaran titik berwarna *yellow* mendapatkan hasil cluster 25 *source* IP *address*, 25 *destination* IP *address*, 15 *source* port, 25 *destination* port, 22 *packet length*, dan 18 *anomaly score* yang dihasilkan dari serangan kategori HTTP *Flood*. Sebaran titik berwarna *orange* merupakan cluster 5 dengan 25 *source* IP *address*, 25 *destination* IP *address*, 21 *source* port, 43 *destination* port, 30 *packet length*, dan 28 *anomaly score*. Sebaran titik berwarna *gold* merupakan cluster 6 dengan 19 *source* IP *address*, 19 *destination* IP *address*, 14 *source* port, 15 *destination* port, 16 *packet length,* dan 16 *anomaly score* dengan *severity level low* dan *attack type* ICMP *Flood*.



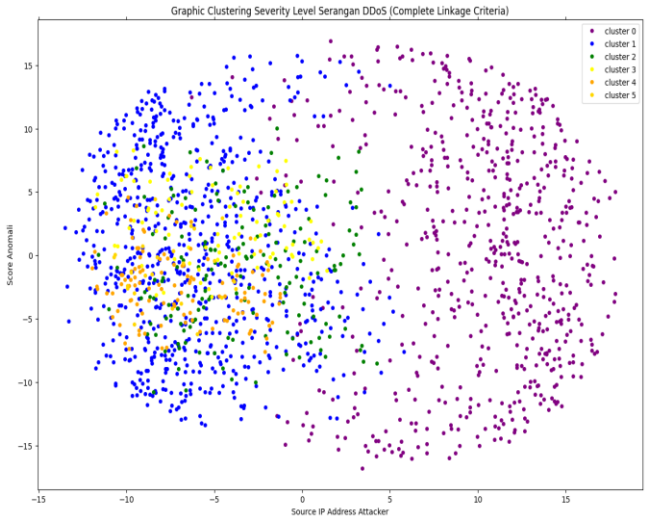
Gambar 7 Pengelompokan Kriteria *Single Linkage* Kategori Serangan

Pada Gambar 7 terdapat sebaran hasil yang berbeda untuk setiap kategori serangan. Setiap koneksi ke suricata yang dimodelkan memiliki motivasi dan target tertentu pada setiap perangkat vServer dan router.

Pengelompokan *Complete Linkage* Berdasarkan Kategori Serangan

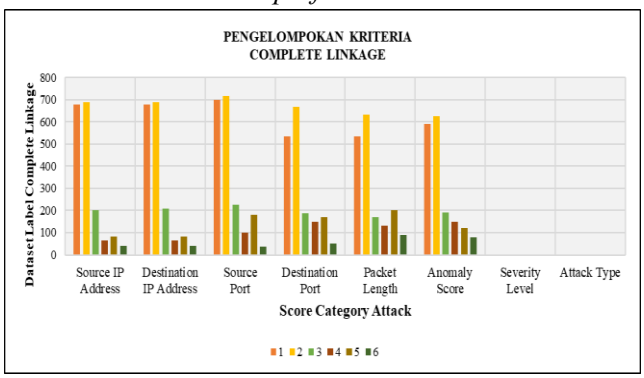
Penyebaran cluster C1, C2, C3, C4, C5 dan C6 dari clustering dataset, ditampilkan pada Gambar 8. Dimana sebaran titik berwarna *purple* (cluster 1) menampilkan dengan kriteria *complete linkage*, dengan kondisi jenis serangan kategori tipe TCP *Sync Flood* dari 680 *source* IP *address* cluster 1 dan *destination* IP *address* sebanyak 680, 700 *source* port, 534 *destination* port, 590 *packet length* dan 590 *anomaly score*. Cluster 1 menghasilkan jumlah *source* IP *address* dengan potensi yang besar dari lalu lintas serangan (*logging* DDoS) tipe protocol TCP *Sync Flood*. Sebaran titik berwarna *blue* pada cluster 2 sebanyak 690 *source* IP *address* dan 690 *destination address*, 718 *source* port, 667 *destination* port, 633 *packet length*, 627 *anomaly score* dengan kategori *severity level high*. Cluster 2 menghasilkan jumlah *source* IP *address* dengan potensi yang besar dari lalu lintas serangan (*logging* DDoS) tipe protocol TCP *Sync Flood*. Cluster 3 membentuk sebaran titik berwarna *light blue* dengan 200 *source* IP *address*, 210 *destination* IP *address*, 225 *source* port, 187 *destination* port, 170 *packet length*, dan 190 *anomaly score* dengan kategori medium dengan tipe serangan HTTP Flood. Cluster 4 dengan sebaran titik berwarna yellow mendapatkan hasil cluster 65 *source* IP *address*, 65 *destination* IP *address*, 100 *source* port, 150 *destination* port, 130 *packet length*, dan 150

anomaly score yang dihasilkan dari serangan kategori HTTP *Flood*. Sebaran titik berwarna *orange* merupakan cluster 5 dengan 83 *source* IP *address*, 83 *destination* IP *address*, 180 *source* port, 170 *destination* port, 200 *packet length*, dan 121 *anomaly score* dengan *severity level* medium dan *attack type* HTTP Flood. Sebaran titik berwarna *gold* merupakan cluster 6 dengan 40 *source* IP *address*, 40 *destination* IP *address*, 36 *source* port, 50 *destination* port, 90 *packet length,* dan 80 *anomaly score* dengan *severity level low* dan *attack type* ICMP *Flood*. Dari masing-masing kategori *attack type* serangan DDoS memiliki karakteristik, hasil analisa anomali yang terjadi dengan HTTP *Flood* penyerang menggunakan *script* otomatis atau tool botnet dengan mengirim permintaan dalam jumlah yang besar melalui protocol HTTP ke perangkat vServer dan vRouter. Dengan kategori *Sync* penyerang mengirimkan permintaan dalam jumlah besar SYN ke vServer. Tipe ICMP Flood digunakan penyerang dengan permintaan dan merespon ICMP *Echo Request/Reply* dengan mengirimkan paket ICMP ke vServer dan vRouter dalam jumlah packet yang besar.



Gambar 8 Grafik Penyebaran Kategori Serangan Kriteria Complete Linkage Serangan

Pada Gambar 32 terdapat sebaran hasil yang berbeda untuk setiap kategori serangan. Setiap koneksi ke suricata yang dimodelkan memiliki motivasi dan target tertentu pada setiap perangkat vServer dan vRouter. Setelah pemeriksaan lebih dekat dari IP sumber, ada sejumlah source IP Address yang muncul lebih sering daripada yang lain pada cluster 1 dan cluster 2, yaitu pada prefix antara lain 57.71.71.107/32, 211.43.37.93/32. Jumlah yang dihasilkan dari cluster 1 680 *source* IP *address* dan cluster 2 terdapat 690 *source* IP *address* jenis kategori serangan dengan *severity level high* dengan *destination* IP *address prefix* 117.103.2.128/29.



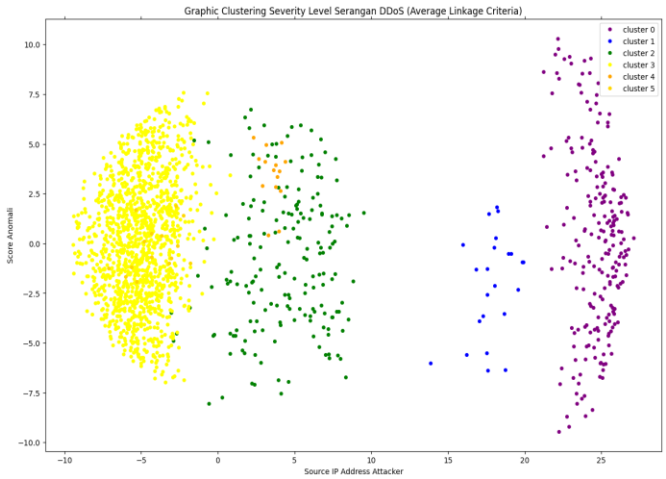
Gambar 9 Pengelompokan Kriteria *Complete Linkage* Kategori Serangan

Pengelompokan *Average Linkage* Berdasarkan Kategori Serangan

Penyebaran *cluster* C1, C2, C3, C4, C5 dan C6 dari *clustering* dataset, ditampilkan pada Gambar 10. Dimana sebaran titik berwarna *yellow* (cluster 4) menampilkan dengan kriteria *average linkage*, dengan kondisi jenis serangan kategori tipe TCP *Sync Flood* dari *source* IP *address* sebanyak 1302, 1302 *destination* IP *address*, 1297 *source port*, 1337 *destination port*, 1337 *packet length* dan 1333 *anomaly score* pada *cluster* 4. Sebaran titik berwarna *purple* pada cluster 1 sebanyak 260 *source* IP *address* dan 271 *destination address*, 274 *source port*, 230 *destination port*, 230 *packet length*, 230 *anomaly score* dengan kategori *severity level high*.

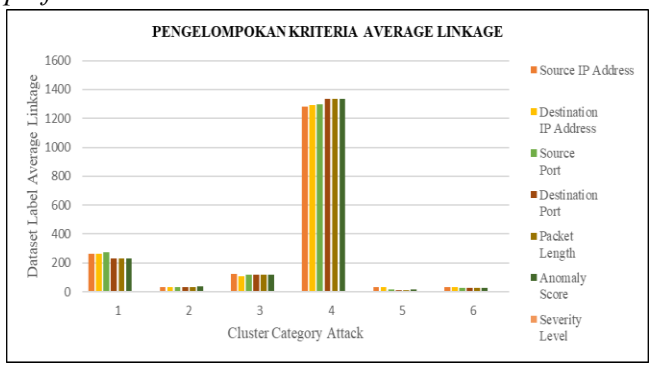
Cluster 2 dengan sebaran titik *blue*, mempunyai 21 *source* IP *address*, 30 *destination* IP *address*, 32 *source port*, 34 *destination port*, 34 *packet length* dan 37 *anomaly score*. Cluster 3 membentuk sebaran titik berwarna *green* dengan 122 *source* IP *address*, 116 *destination* IP *address*, 117 *source port*, 119 *destination* port, 119 *packet length*, dan 118 *anomaly score* dengan kategori medium dengan tipe serangan HTTP *Flood*. Cluster 4 dengan sebaran titik berwarna *yellow* mendapatkan hasil *cluster* 1302 *source* IP *address*, 1302 *destination* IP *address*, 1297 *source port*, 1337 *destination port*, 1337 *packet length*, dan 1333 *anomaly score* yang dihasilkan dari serangan kategori HTTP *Flood* dan dengan kategori *severity level high*. Sebaran titik berwarna *orange* merupakan *cluster* 5 dengan 14 *source* IP *address*, 15 *destination* IP *address*, 14 *source port*, 13 *destination port*, 13 *packet length*, dan 15 *anomaly score* dengan *severity* level medium dan *attack type* HTTP *Flood*. Sebaran titik berwarna *gold* merupakan *cluster* 6 dengan 29

source IP *address*, 24 *destination* IP *address*, 30 *source port*, 24 *destination port*, 25 *packet length*, dan 25 *anomaly score* dengan *severity level low* dan *attack type* ICMP *Flood*. Dari masing-masing kategori *attack type* serangan DDoS memiliki karakteristik, hasil analisa anomali yang terjadi dengan ICMP *Flood*.



Gambar 10 Grafik Penyebaran Kategori Serangan Kriteria *Average Linkage* Serangan

Pada Gambar 11 terdapat sebaran hasil untuk setiap kategori serangan. Setiap koneksi ke suricata yang dimodelkan memiliki motivasi dan target tertentu pada setiap perangkat vServer dan vRouter. Setelah pemeriksaan lebih dekat dari IP sumber, ada sejumlah source IP *address* yang muncul lebih sering daripada yang lain pada cluster 4, cluster 1 dan cluster 3, yaitu pada prefix antara lain 92.192.73.229/32, 43.213.82.40/32. Jumlah yang dihasilkan dari cluster 4 990 *source* IP *address* dan cluster 3 terdapat 384 *source* IP *address* jenis kategori serangan dengan *severity level high* dengan destination IP Address *prefix* 117.103.2.128/29.

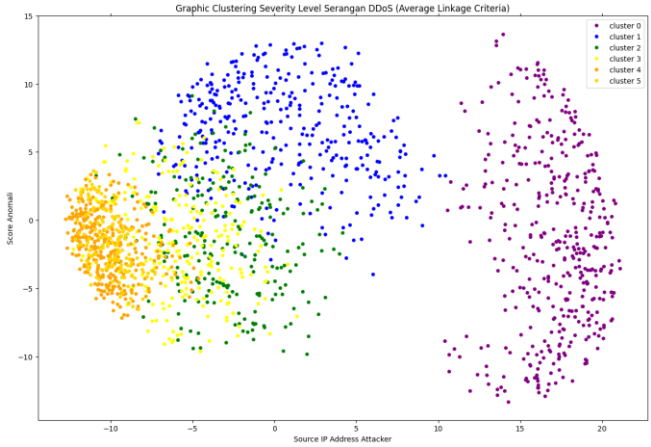


Gambar 11. Kriteria Average Linkage Kategori Serangan

Pengelompokan *Ward Linkage* Berdasarkan Kategori Serangan

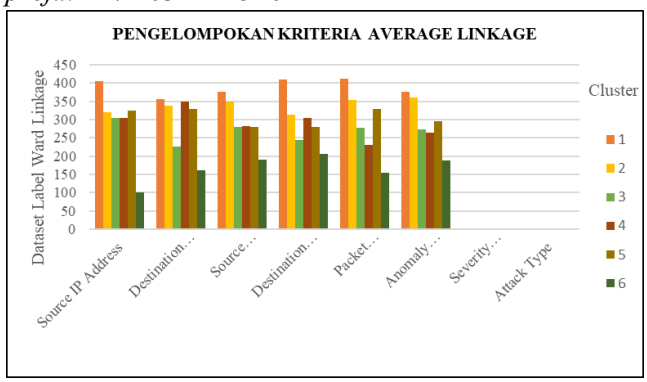
Pengelompokan yang dilakukan dengan metode ward linkage, bertujuan untuk mengetahui hasil deteksi dan anomali dari *policy* dan *rules* yang dikonfigurasi pada *suricata.yaml* pada monitoring perangkat vServer dan router, untuk menggabungkan dua kelompok atribut dan variabel dataset yang akan memiliki dampak minimum pada peningkatan jumlah variabel dalam dataset log suricata.

Penyebaran *cluster* C1, C2, C3, C4, C5 dan C6 dari *clustering* dataset, ditampilkan pada Gambar 49. Dimana sebaran titik berwarna *purple* (cluster 1) menampilkan dengan kriteria *ward linkage*, dengan kondisi jenis serangan kategori tipe TCP *Sync Flood* dari 435 *source* IP *address*, 380 *destination* IP *address*, 375 *source port*, 425 *destination port*, 412 *packet length* dan 377 *anomaly score* pada *cluster* 1. Sebaran titik berwarna *blue* pada *cluster* 2 sebanyak 330 *source* IP *address* dan 335 *destination address*, 350 *source* port, 320 *destination port*, 412 *packet length*, 377 *anomaly score* dengan kategori *severity level high*. Cluster 3 membentuk sebaran titik berwarna *green* dengan 295 *source* IP *address*, 225 *destination* IP *address*, 200 *source port*, 225 *destination* port, 330 *packet length*, dan 361 *anomaly score* dengan kategori *high* dengan tipe serangan HTTP *Flood*. Cluster 4 dengan sebaran titik berwarna *yellow* mendapatkan hasil *cluster* 305 *source* IP *address*, 350 *destination* IP *address*, 210 *source port*, 315 *destination port*, 330 *packet length*, dan 361 *anomaly score* yang dihasilkan dari serangan kategori HTTP *Flood*. Sebaran titik berwarna *orange* merupakan *cluster* 5 dengan 315 *source* IP *address*, 335 *destination* IP *address*, 280 *source port*, 280 *destination port*, 330 *packet length*, dan 361 *anomaly score* dengan *severity* level medium dan *attack type* HTTP *Flood*. Sebaran titik berwarna *orange* merupakan *cluster* 6 dengan 170 *source* IP *address*, 160 *destination* IP *address*, 190 *source port*, 205 *destination port*, 155 *packet length*, dan 188 *anomaly score* dengan *severity level low* dan *attack type* ICMP *Flood*. Dari masing-masing kategori attack type serangan DDoS memiliki karakteristik, anomali *logging* mengirim permintaan dalam jumlah yang besar melalui protocol HTTP ke perangkat vServer dan vRouter. Dengan kategori *Syn* penyerang mengirimkan permintaan dalam jumlah besar SYN ke vServer.



Gambar 12 Penyebaran Kategori Serangan Kriteria *Ward Linkage* Serangan

Pada Gambar 13 terdapat sebaran hasil yang berbeda untuk setiap kategori serangan. Setiap koneksi ke suricata yang dimodelkan memiliki motivasi dan target tertentu pada setiap perangkat vServer dan vRouter. Setelah pemeriksaan lebih dekat dari IP sumber, ada sejumlah *source* IP Address yang muncul lebih sering daripada yang lain pada cluster 1, cluster 2 dan cluster 3, yaitu pada prefix 208.69.237.108/32, 212.122.222.54/32. Jumlah yang dihasilkan dari *cluster* 1 435 *source* IP *address* dan *cluster* 2 terdapat 330 *source* IP *address* jenis kategori serangan dengan *severity level high* dengan *destination* IP *address prefix* 117.103.2.128/29.



Gambar 13 Pengelompokan Kriteria Ward Linkage Kategori Serangan

Mitigasi Firewall IPSet File (*Block source IP Address from a File*)

Firewall IPSet File diimplementasikan untuk membuat file database target dengan mekanisme menambahkan entri *source* IP *address* yang ditetapkan otomatis berdasarkan *rules ipset file*. sintaks *ipset file* akan melakukan entri secara otomatis untuk memblokir semua *source* IP *address* yang diinput pada file dari hasil pengelompokan *hierarchical clustering* dataset berdasarkan *severity level rules* dan *policy* yang sudah ditentukan. Daftar *source* IP *address rules ipset file* yang digunakan untuk teknik mitigasi pada penelitian ini ditunjukkan pada sintaks gambar 14 berikut.

```
1#!/bin/bash
echo "### Source-IP-Address-Drop-From-File."
#File that contains the Ips and Nets to block
FILE=" Source-IP-Address-Deny.txt"
ipset -N bad_hosts iphash -exist
# Flushing the set if it exists
ipset -F bad_hosts
echo "Adding Ips from $FILE to bad_hosts set:"
for ip in `cat $FILE`
do
ipset -A bad_hosts $ip
echo -n "$ip "
Done
echo -e -n "\nDropping with iptables... "
ptables -I INPUT -m set -match-set bad_hosts src -j DROP
echo "Done"
```

Gambar 14 Firewall IPSet File (*Block source IP Address from a File*)

- Instalasi ipset file dengan baris sintaks `apt install ipset`.
- Kemudian membuat file `source-IP-address-drop.txt`. File txt ini akan didaftarkan *source* IP address dengan kriteria anomali berdasarkan hasil *clustering*.

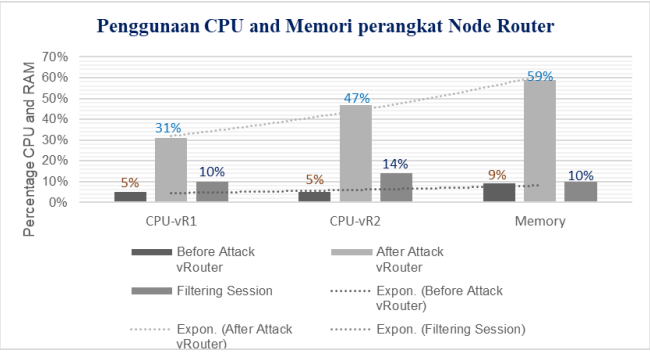
```
#!/bin/bash
        echo -n 'Enter the Prefix Source IP Address: '
read IP
        echo -n 'Enter Blocked or Accept Address'
read ANSWER
if [ $ANSWER = "DROP" ]
then
iptables -I INPUT -s $IP -j DROP
        echo "Traffic from $ source IP Address has beed blocked"
elif [ $ANSWER = "ACCEPT"]
then
iptables -I INPUT -s $IP -j ACCEPT
        echo "Traffic from $IP has beed accepted"
else
        echo "Invalid option. Enter DROP or ACCEPT"
fi

#!/bin/bash
if [$# -eq 2]
then
        echo "Blocking $1 port $2"
        iptables -I INPUT -p $1 --sport $2 -j DROP
        echo "Done"

else
        echo"This Script was Run with Number Port TCP/UDP of Arguments"
fi
```

Gambar 15 Firewall *Scripting*

Aturan yang digunakan untuk *firewall scripting* adalah *automation shell script* yang mempunyai *rule* untuk menambahkan, menghapus dan memodifikasi *rules* firewall, termasuk *accept* atau *drop*. Pada penelitian ini *firewall script* digunakan untuk membuat aturan pada port yang akan diblokir. Tahapan untuk membuat rules firewall akan disesuaikan dengan dataset yang sudah didaftarkan dari log dataset *clustering*. Aturan yang dibuat pada *firewall scripting* adalah *header* paket *protocol port* berdasarkan *source port*. Pembuatan nama *file* untuk masing-masing aturan adalah `drop_source_port.sh`, untuk membuat aturan *action* `drop`. Berikut baris sintaks untuk firewall *scripting* berdasarkan *source port*.

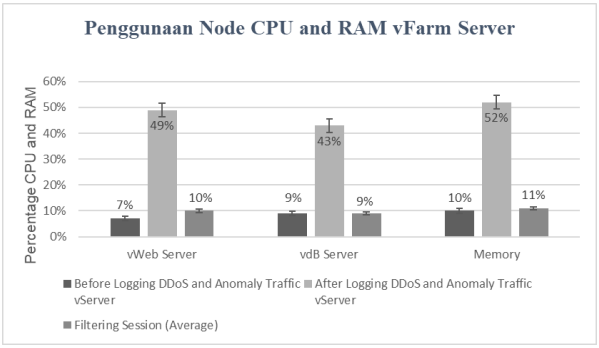
Pengujian penggunaan kapasitas vCPU dan memori dari teknik mitigasi yang dilakukan, diujikan

untuk perangkat router. Gambar 16 merupakan grafik sebelum terjadi koneksi DDoS keperangkat router, sumber daya vCPU pada perangkat router menampilkan beban kerja vCPU vR1 5%, vCPU vR2 5% dan memory 9%. Pada masing-masing perangkat route ini tidak ada konfigurasi khusus hanya *default config* route agar terlihat sumber daya dan beban kerja tidak *load* selama proses terkoneksi ke jaringan public. Dari hasil monitoring selama eksperimen, perangkat router yang *facing* ke internet tanpa adanya filtering ini, dan dari hasil anomali terutama untuk *source* IP *address* dan *source* port terlihat status vRouter load vCPU, mengalami peningkatan, vCPU vR1 31%, vCPU vR2 47% dan memory 24%. Peningkatan sumber daya vCPU dan memori akibat adanya lalu lintas konektivitas di perangkat router yang tidak difilter, yang berasal dari jaringan public internet. Setiap paket masuk *in* dan *out* yang melewati perangkat router akan diproses CPU. Gambar 16 terlihat bahwa histori beban kerja dari sumber daya vCPU mengalami penuruan persentasi vCPU vR1 10%, vCPU vR2 14% dan memory 10%.



Gambar 16 Penggunaan Beban Kerja CPU dan Memori Perangkat Router

Gambar 17 menampilkan beban kerja vCPU vWebServer 7%, vCPU vdBServer 9% dan memori 10%. Dari hasil anomali terutama untuk *source* IP *address* dan *source* port terlihat status vServer load vCPU, mengalami peningkatan, vCPU vWebServer 49%, vCPU vdBServer 43% dan memori 52%. Peningkatan sumber daya vCPU dan memori akibat adanya lalu lintas konektivitas di perangkat node vServer yang tidak ada *filtering*. Setiap paket masuk *in* dan *out* yang melewati perangkat vServer akan diproses vCPU. Tanpa adanya filter yang yang diterapkan pada perangkat vServer, terutama pada interface bridge vServer harus menangani semua paket *in* dan *out*. Setelah konvergensi *rule* firewall IPSet dan firewall *scripting* dalam status running dan aktif, pada Gambar 48 terlihat bahwa histori beban kerja dari sumber daya vCPU mengalami penuruan persentasi vCPU vR1 10%, vCPU vR2 9% dan memory 11%.



Gambar 17 Penggunaan Beban Kerja CPU dan Memori Perangkat vServer

KESIMPULAN

Hasil penelitian yang diimplementasikan menunjukkan bahwa teknik *clustering* dan mitigasi secara efektif mengidentifikasi dan mengatasi serangan DDoS yang menargetkan perangkat router dan vServer. Dengan clustering *single linkage*, *complete linkage*, *average linkage*, dan *ward linkage*, berhasil mengidentifikasi beberapa cluster yang merepresentasikan berbagai tingkat ancaman berdasarkan lalu lintas IP *source* dan IP *destination*. Hasil dari penelitian ini menunjukkan bahwa cluster dengan intensitas serangan tinggi, seperti *TCP SYN Flood*, dapat terdeteksi sehingga memungkinkan penanganan yang lebih tepat dan terarah terhadap potensi ancaman pada perangkat router dan vServer. Mitigasi menggunakan IPSet dan firewall *scripting* IPTables terbukti efektif untuk mengurangi dampak dari serangan DDoS pada perangkat. Sebelum penerapan mitigasi firewall, dengan perangkat langsung terhubung ke jaringan publik mengalami peningkatan beban kerja signifikan. Setelah kebijakan firewall diterapkan, pada perangkat terjadi penurunan vCPU sebesar 10% sampai 14% dan pengurangan memori hingga 11%, hasil ini menunjukkan bahwa perangkat dapat lebih stabil dan responsif terhadap ancaman.

UCAPAN TERIMA KASIH

Penulis mengucapkan terima kasih kepada DRPPM Universitas Budi Luhur atas dukungan dan sumber pendanaan penelitian dengan Nomor K/UBL/FTI/000/004/09/23 pada tahun 2023.

DAFTAR PUSTAKA

Abdullayeva, F. J. (2022). Distributed denial of service attack detection in E-government cloud via data clustering. *Array*, *15*(December 2021), 100229.

Adedeji, K. B., Abu-Mahfouz, A. M., & Kurien, A. M. (2023). DDoS Attack and Detection Methods in Internet-Enabled Networks: Concept, Research Perspectives, and Challenges. *Journal of Sensor and Actuator Networks*, *12*(4).

Alzahrani, R. J., & Alzahrani, A. (2021). Security analysis of ddos attacks using machine learning algorithms in networks traffic. *Electronics (Switzerland)*, *10*(23).

Damanik, H. A. (2022). Securing Data Network for Growing Business VPN Architectures Cellular Network Connectivity. *Acta Informatica Malaysia*, *6*(1), 01–06.

Damanik, H. A., & Anggraeni, M. (2018, December 25). *Teknik Pengujian Keamanan Data Text Bertingkat Dengan Metode Steganography LSB dan Teknik Enkripsi | Jurnal Penelitian Pos dan Informatika*.

Damanik, H. A., & Anggraeni, M. (2024). *Pola Pengelompokan dan Pencegahan Public Honeypot menggunakan Teknik K-Means dan Automation Shell-Script*. *12*(1), 65–79.

Damanik, H. A., Anggraeni, M., & Nusantari, F. A. A. (2023). *Konsep dan Penerapan Switching dan Routing Implementasi Jaringan Komputer Berbasis Cisco*. CV. Mega Press Nusantara.

Faiz, M. N., Somantri, O., & Muhammad, A. W. (2022). Machine Learning-Based Feature Engineering to Detect DDoS Attacks. *Jurnal Nasional Teknik Elektro Dan Teknologi Informasi |*, *11*(3), 176–182.

Gupta, A. (2018). Distributed Denial of Service Attack Detection Using a Machine Learning Approach. *Calgary, Alberta*, (April).

Haseeb-ur-rehman, R. M. A., Aman, A. H. M., Hasan, M. K., Ariffin, K. A. Z., Namoun, A., Tufail, A., & Kim, K. H. (2023). High-Speed Network DDoS Attack Detection: A Survey. *Sensors*, *23*(15).

Huang, C., Han, J., Zhang, X., & Liu, J. (2019). Automatic identification of honeypot server using machine learning techniques. *Security and Communication Networks*, *2019*.

Jasim, M. N., & Gaata, M. T. (2022). K-Means clustering-based semi-supervised for DDoS attacks classification. *Bulletin of Electrical Engineering and Informatics*, *11*(6), 3570–3576.

Jose, S., Malathi, D., Reddy, B., & Jayaseeli, D. (2018). A Survey on Anomaly Based Host Intrusion Detection System. *Journal of Physics: Conference Series*, *1000*(1).

May, A., & Koay, Y. (2019). *Detecting High and Low Intensity Distributed Denial of Service (DDoS) Attacks*. 1–188.

Patel, M. (2020). *Demilitarized Zone An Exceptional Layer of Network Security to Mitigate DDoS Attack*. 62.

Praptodiyono, S., Firmansyah, T., Anwar, M. H., Wicaksana, C. A., Pramudyo, A. S., & Al-Allawee, A. (2023). Development of Hybrid Intrusion Detection System Based on Suricata With Pfsense Method for High Reduction of Ddos Attacks on Ipv6 Networks. *Eastern-European Journal of Enterprise Technologies*, *5*(9(125)), 75–84.

Putri, N. A., Stiawan, D., Heryanto, A., Septian, T. W., Siregar, L., & Budiarto, R. (2017). Denial of service attack visualization with clustering using K-means algorithm. *ICECOS 2017 - Proceeding of 2017 International Conference on Electrical Engineering and Computer Science: Sustaining the Cultural Heritage Toward the Smart Environment for Better Future*, 177–183.

Shah, S. A. R., & Issac, B. (2018). Performance comparison of intrusion detection systems and application of machine learning to Snort system. *Future Generation Computer Systems*, *80*, 157–170.

She, C., Wen, W., Zheng, K., & Lyu, Y. (2016). *Application-Layer DDoS Detection by K-means Algorithm*. *50*(Iceeecs), 75–78.

Shutaywi, M., & Kachouie, N. N. (2021). Silhouette analysis for performance evaluation in machine learning with applications to clustering. *Entropy*, *23*(6), 1–17.

Vanin, P., Newe, T., Dhirani, L. L., O'Connell, E., O'Shea, D., Lee, B., & Rao, M. (2022). A Study of Network Intrusion Detection Systems Using Artificial Intelligence/Machine Learning. *Applied Sciences (Switzerland)*, *12*(22).

Yamamoto, Y., & Yamaguchi, S. (2023). Defense Mechanism to Generate IPS Rules from Honeypot Logs and Its Application to Log4Shell Attack and Its Variants. *Electronics*, *12*(14), 3177.