ANALISIS DAN PERANCANGAN *PRIVATE CLOUD STORAGE* MENGGUNAKAN METODE PENGAMANAN *IDS* (*INTRUSION DETECTION SYSTEM)* DAN *IPS*(*INTRUSION PREVENTION SYSTEM*) (STUDI KASUS: DISKOMINFO KOTA PADANG PANJANG)

Irzon Meiditra[1], Yuhandri[2], Sumijan[3]

[1]Universitas Putra Indonesia YPTK Padang
Email: [1]meiditrairzon@gmail.com, [2]yuhandri.yunus@gmail.com, [3]sumijan@upiyptk.ac.id

Abstrak: Dinas komunikasi dan informatika Kota Padang Panjang merupakan unsur pelaksana urusan pemerintah dibidang komunikasi,informatika,persandian dan statistic dan mempunyai tugas menyelenggarakan urusan pemerintah di bidang komunikasi dan informatika. Dan di Dinas komunikasi dan informatika memnpunyai layanan penyimpanan server dengan banyaknya data pengembangan server cloud computing akan menjadi solusi. Cloud computing merupakan bentuk kemajuan teknologi yang telah berkembang seiring dengan kemajuan zaman, hal ini memacu dalam penggunaan internet yang semakin meningkat. Menggunakan teknologi internet yang mampu menerapkan server bersifat virtual/online, yang mempunyai tujuan membangun server cloud computing di Dinas Komunikasi dan Informatika Kota Padang Panjang Operating System (OS) Proxmox VE (Virtual Environment).*Cloud computing* merupakan bentuk kemajuan teknologi yang telah berkembang seiring dengan kemajuan zaman, hal ini memacu dalam penggunaan internet yang semakin meningkat. Dengan menggunakan teknologi internet yang mampu menerapkan server bersifat virtual/online, yang mempunyai tujuan membangun s*erver cloud computing* di Dinas Komunikasi dan Informatika Kota Padang *Panjang Operating System (OS) Proxmox VE (Virtual Environment) 6.4*. *Cloud computing* mampu menyediakan layanan penyimpanan yang bisa digunakan secara bersamaan. Hasil penelitian ini menghasilkan sebuah server *cloud Storage* yang menerapkan sistem keamanan dengan metode *ids (intrusion detection system)* dan *ips (intrusion prevention system)* yang mampu melakukan proses penyimpanan data *(storage)*, menggunakan *software* secara bersamaan dalam jaringan, serta penggunaan insfrastruktur dalam ruang lingkup jaringan *cloud computing* di Dinas Komunikasi dan Informatika Kota Padang Panjang dengan menggunakan model layanan *private cloud Storage*.

Kata kunci*:* Cloud Computing,Vmware, Proxmox, Ids, Ips

Abstract:*The Office of Communication and Informatics of the City of Padang Panjang is an executive element of government affairs in the field of communication, informatics, coding and statistics and has the task of carrying out government affairs in the field of communication and informatics. And the Communication and Informatics Office has a server storage service with lots of data. The development of a cloud computing server will be a solution. Cloud computing is a form of technological progress that has developed along with the times, this has spurred the increasing use of the internet. Using internet technology that is capable of implementing virtual/online servers, which has the goal of building a cloud computing server at the Padang Panjang City Communication and Information Service Operating System (OS) Proxmox VE (Virtual Environment). Cloud computing is a form of technological progress that has developed along with progress of the times, this spurred the use of the internet which is increasing. By using internet technology that is capable of implementing virtual/online servers, the aim is to build a cloud computing server at the Padang Panjang City Communication and Information Service Operating System (OS) Proxmox VE (Virtual Environment) 6.4. Cloud computing is able to provide storage services that can be used simultaneously. The results of this study produce a cloud Storage server that implements a security system using the ids (intrusion detection system) and ips (intrusion prevention system) methods that is capable of carrying out data storage processes (storage), using software simultaneously in the network, and using infrastructure within the scope of cloud computing network at the Padang Panjang City Communication and Information Service using the private cloud Storage service model.*

Keyword: *Cloud Computing, Vmware, Proxmox, Ids, Ips*

1. PENDAHULUAN

Internet adalah sebuah interkoneksi dengan skala yang luas yang dapat menghubungkan antar perangkat lain dengan perangkat lainnya di seluruh dunia selama terhubung dengan koneksi internet. Internet juga berguna untuk menambah wawasan ilmu pengetahuan,menghubungkan setiap individu ataupun setiap instansi Menurut Speedtest pada speedtest.net/global indeks/indonesia yang di akses Juli 2022 bahwa diketahui kecepatan rata-rata internet di indonesia untuk data seluler untuk unduh berada di 25.47Mbps dan unggah berada di 12.99Mbps, Sedangkan untuk internet kabel memiliki kecepatan rata-rata untuk unduh berada 33.65Mbps dan sedangkan untuk unggahnya berada di 23.43Mbps. [1]

Cloud Computing merupakan teknologi baru yang sedang ramai dibahas oleh para pakar dan pengguna teknologi informasi. Teknologi cloud computing dihadirkan sebagai upaya untuk memungkinkan akses sumber daya dan aplikasi dari mana saja melalui jaringan Internet. [2]. Cloud computing memiliki kelebihan seperti memberikan berbagai pilihan model layanan, jenis penyimpanan data, serta pengaturan komputasi yang sesuai kebutuhan sehingga memberikan manfaat yang menarik yaitu efisiensi, efektif dan hemat biaya. [3]

4 definisi terkait dalam mengenai model karakteristik yaitu : Public Cloud digunakan atau dipakai secara bersama-sama (multi-tenancy), Private Cloud diimplementasikan untuk memenuhi kebutuhan dari suatu organisasi maupun perusahaan tertentu secara khusus, Hybrid Cloud menggabungkan dari layanan dua infrastruktur, yaitu layanan cloud Public dan Cloud Private yang biasanya diimplementasikan oleh suatu organisasi ataupun perusahaan, merupakan sistem operasi mesin virtual yang mulai banyak dipakai oleh para pengguna teknologi virtualisasi. [4]

Cloud storage memiliki keunggulan skalabilitas penggunaan storage yang dapat disesuaikan dengan kebutuhan dari sisi pengguna. [5]. Hasil dari penelitian adalah menggunakan metode IDS (Intrusion Detection System) dan IPS (Intrusion Prevention System) membangun sebuah sistem keamanan data pada komputer FTP server. [6].

Hasil penelitian Intrusion Prevention System merupakan salah satu tool pengamanan pada jaringan, IPS sebagai untuk melindungi webserver dari serangan SQL Injection menggunakan SQLMap. [7].Menggunakan metode Intrusion Detection System dan Decision Tree dapat simpulkan bahwa IDS akan menganggap adanya anomali jika paket perdetik serangan yang didapat melebihi [8] menggunakan metode Instrusion Detection System menunjukkan Network Forensic Investigation Framework memudahkan proses investigasi ketika terjadi serangan jaringan.[9]

Menggunakan Seleksi Fitur dan Firebase Cloud Messaging dan Intrusion Detection System merupakan salah satu bagian yang mendasar dari sebuah alat keamanan Jaringan komputer dapat dimanfaatkan oleh para pengguna komputer didalam melakukan pertukaran data tanpa harus beranjak dari tempat duduknya dalam satu kesatuan. [10] Firewall dapat berupa perangkat keras, perangkat lunak, atau antara dua komputer atau lebih. [11]

Proxmox VE adalah platform virtualisasi yang lebih lengkap karena dapat melakukan backup virtual machine. Serta Proxmox VE mampu mengefisiensikan unit fisik komputer server dengan menggunakan teknologi virtualisasi, Virtualisasi/ Virtualization adalah sebuah teknik atau cara untuk membuat sesuatu dalam bentuk virtualisasi. [12] Snort merupakan sebuah perangkat lunak yang berfungsi untuk mengamati aktifitas dalam suatu jaringan computer. [13]

Penelitian terkait desain topologi jaringan pernah dilakukan untuk perancangan dan pengembangan jaringan VLAN pada Dili Institute of Technologi (DIT) Timor Leste. Pada penelitian ini memfokuskan tentang bagaimana meningkatkan performansi jaringan dari beberapa divisi yang saling terpisah dengan membandingkan dua buah model jaringan. Uji coba penelitian ini menggunakan perkakas bantu berupa aplikasi packet tracer, dimana aplikasi ini memungkinkan untuk merancang sebuah jaringan besar secara virtual dengan detail pengalamatan (addressing) komputer. Hasil dari penelitian ini menunjukkan konfigurasi VLAN dengan menggunakan metode trunking switch yang dihubungkan dengan router dapat meningkatkan performansi jaringan. [14]

Dinas komunikasi dan informatika kota padang Panjang merupakan unsur pelaksana urusan pemerintahan bidang komunikasi dan informatika, urusan pemerintahan bidang persandian, dan urusan pemerintahan bidang statistik yang dipimpin oleh Kepala Dinas yang berkedudukan di bawah dan

bertanggung jawab kepada Bupati melalui Sekretaris Daerah. Permasalahan yang sering terjadi di dinas kounikasi dan informatika adalah terlalu overload server,karna server yang masih berbentuk fisik sedangkan dengan adanya proxmox sebagai software dan untuk membuat cloud computing dengan server berbasis online atau virtualisasi. Berdasarkan uraian yang telah dijelaskan dan diulas penelitian terdahulu diatas, maka penulis mengajukan suatu penelitian dengan judul "Analisis dan perancangan private cloud storage menggunakan IDS (Intrusion Detection System) dan IPS(Intrusion Prevention System) (Studi Kasus di dinas komunikasi dan informatika kota padang panjang)"

Metode Intrusion Detection System merupakan teknik khusus yang dapat digunakan seorang admin jaringan komputer yang bertanggung jawab untuk mengamankan akses jaringan komputer dari penyusup (intruder) yang sedang melakukan sistem detection system adalah sebuah perangkat keamanan siber yang memantau lalu lintas di jaringan komputer. Perangakat ini menganalisis lalu lintas paket data dalam jaringan. Jika terjadi pola yang cocok dengan serangan yang diketahui. Metode IDS ini digunakan untuk dapat mengetahui atau mendeteksi adanya aktivitas jaringan oleh pengguna tertentu atau attacker yang aktivitasnya dianggap mencurigakan (sniffing) Kerja IPS yaitu Menentukan IPTables dan menentukan Rules IPTables bekerja secara real time, dan merupakan sistem perlindungan aktif seperti IDS, ia mencoba mengidentifikasi potensi ancaman berdasarkan fitur pemantauan dari host atau jaringan yang dilindungi dan dapat menggunakan metode deteksi tanda tangan, anomali, atau hibrid.

Tahap ini akan mengkonfigurasikan IPTables dengan linux ubuntu secara virtual pada Vmware workstation denga mengupdate dan mengupgrade karena pada sistem operasi maka akan mendapat instalasi paket pendukung dan konfigurasi rules IPTables dengan menjalankan sudo apt-get install iptables-persistent-y dan melihat kondisi konfigurasi yang berlaku pada IPTables yaitu iptables-L-v.

1. **Menentukan Rules IPTables**

   Perancangan rules pada tabel pengaturan paket, iptables memiliki beberapa tabel yang berfungsi untuk menentukan data. Setiap tabel tersebut memiliki rules atau kumpulan aturan rules pada Snort terdapat dua bagian yang harus diperhatikan yaitu bagian header and option rules. Aturan-aturan pada rule header berfungsi sebagai tindakan apa yang harus dilakukan, misalnya memantau protokol tertentu, alamat IP asal dan alamat IP tujuan, dan nomor port asal dan tujuan. Pada action field yang terdapat pada header rule yang memiliki tiga property yaitu, alert, log, dan pass. Protocol field bertindak sebagai kriteria untuk mendeteksi data traffic yang masuk dalam jaringan, protokol yang dideteksi bisa mencakup port IP, TCP, UDP, maupun port ICMP. Aturan pada Snort juga terdapat IP address sumber dan IP address tujuan. Direction field ditulsikan dengan yang menjelaskan arah data raffict jaringan antara komputer sumber dan komputer tujuan. Port field menjelaskan mengenai kriteria dalam aturan Snort untuk menentukan protocol port mana yang digunakan. Lebih lanjut, jika ingin menentukan setiap port, field dari port tersebut didefinisikan dengan penulisan rule options berfungsi untuk menampilkan pesan-pesan yang akan ditampilkan dan juga untuk menentukan paket seperti apa yang nantinya harus diamati. Fitur options rule memiliki dua bagian utama yaitu, keyword dan argument yang dituliskan di dalam tanda kurung "()" dan dipisahkan dengan titik koma ";". Keyword options dipisahkan dari argumen dengan titik dua ":". Sedangkan untuk rules Snort sendiri dapat memiliki lebih dari satu opsi dalam rule options. Contoh keyword options adalah msg, ttl, tos, dan icode.

Tabel 2.1 Menentukan *Rules IPTables*

No	Perintah	Keterangan
1.	*Iptables-P INPUT ACCEPT*	Memblokir semua paket data secara default
2.	*iptables -A INPUT -I eth32-j ACCEPT*	aturan atau *rules* dapat memasukan semua paket data secara default membuka *interface*
3.	*iptables -A INPUT -I eth32-j ACCEPT*	aturan atau *rules* dapat memblokir semua paket data secara default membuka *interface*
4.	*Iptables -A INPUT -s 192.168.59.128 -j DROP*	Akan menambahkan aturan dibaris terakhir paket data yang akan ditambahkan
5.	*Iptables -A FORWARD -s 192.168.59.128 -j DROP*	Komputer linuxnya berfungsi sebagai router dan tidak menggunakan tabel INPUT
3.	*iptables -I INPUT -s 192.168.59.129 -j ACCEPT*	Untuk memberikan hak akses kepada sever IDS dan IPS
4.	*iptables -I INPUT -s* 192.168.1.1/24 *-j ACCEPT*	Menginputkan ip pada rules Kepala Sub bagian Keuangan Perencanaan,evaluasi,dan Pelaporan
5.	*iptables -I INPUT -s* 192.168.1.3/24 *-j ACCEPT*	Menginputkan ip pada rules Kepala Sub Bagian Umum dan Kepegawaian

6.	*iptables -I INPUT -s* 192.168.1.4/24 *-j ACCEPT*	Menginputkan ip pada rules Kepala Seksi Statistik
7.	*iptables -I INPUT -s* 192.168.1.5/24 *-j ACCEPT*	Menginputkan ip pada rules Kepala Seksi layanan aplikasi
8.	*iptables -I INPUT -s* 192.168.1.6/24 *-j ACCEPT*	Menginputkan ip pada rules Kepala Seksi Infrastruktur Teknologi dan persandian
9.	*iptables -I INPUT -s* 192.168.8.7/24 *-j ACCEPT*	Menginputkan ip pada rules KepalaSeksidokumentasidan hubungan media
10	*iptables -I INPUT -s* 192.168.12.8/24 *-j ACCEPT*	Menginputkan ip pada rules KepalaSeksipengelolaan informasi publik
11	*iptables -I INPUT -s* 192.168.12.15/24 *-j ACCEPT*	Menginputkan ip pada rules Kepala Seksi pengelolaan komunikasi publik

2. Perancangan Serangan Server Cloud dengan Port Scanning

Port Scanning merupakan serangan yang dilakukan untuk mendapatkan informasi port mana yang terbuka. Serangan ini dapat memungkinkan tindakkan penyerang untuk memonitoring target tujuan dan penyerang dapat menganalisa setiap data yang terhubung dengan penyerang. Secara umum serangan port scanning biasa dilakukan menggunakan aplikasi nmap untuk mendapatkan hasil yang maksimal. serangan terhadap suatu sistem yang dilakukan untuk mendapatkan informasi port yang terbuka dengan menggunakan IP address, pada penelitian ini akan dilakukan port scanning terhadap alamat IP server cloud yaitu 192.168.59.128/24 dalam hal ini attacker melakukan scanning pada system menggunakan nmap untuk mengetahui port apa saja yang terbuka dan services apa yang berjalan didalamnya dapat dilihat pada tabel.

Tabel 2.2 Perancangan Serangan Server Cloud dengan Port Scanning

No	IP Adress	PROTOCOL	PORT
1.	192.168.59.128	TCP	22
2.	192.168.59.128	TCP	111
3.	192.168.59.128	TCP	3128
4.	192.168.59.128	TCP	6789
5.	192.168.59.128	TCP	3300

3. *Perancangan Security Menggunakan IPS (Intrusion Prevention System)*

Sistem keamanan pada komputer menggunakan IDS dan IPS menggunakan Snort dan portsentry. Sistem IDS menggunakan Snort bekerja dengan melakukan monitoring paket yang melintas dalam jaringan. Kemudian Snort akan memeriksa setiap paket yang masuk melalui traffic jaringan dengan database rule Snort. Traffic tersebut kemudian dibandingkan dengan rules Snort, jika pada traffic jaringan terdeteksi adanya ancaman, maka Snort akan menampilkan pesan peringatan (alert) real-time pada admin melalui tulisan pesan pada layar komputer Pada perancangan peneltian ini akan mengkonfigurasikan sebuah system yang memiliki kemampuan untuk memonitoring jaringan,mendeteksi adanya aktifitas yang mencurigakan didalam suatu jaringan yang dianggap sebagai serangan penyusupan dan melakukan pencegahan terhadap serangan penyusupan tersebut (Intrusion Prevention System), Perancangan system terdiri dari server dan client yang disatukan dalam satu jaringan yang sama.Laporan hasil perangkingan.

Snort adalah NIDS yang bekerja dengan menggunakan signature detection, berfungsi juga sebagai sniffer dan packet logger. Snort pertama kali di buat dan dikembangkan oleh Marti Roesh, lalu menjadi sebuah opensource project. Versi komersial dari snort dibuat oleh Sourcefire. Snort merupakan suatu tools paket instalasi sistem linux, yang fungsi utamanya dapat digunakan untuk mendeteksi adanya penyusup (threats). Selain itu Snort mampu menganalisis paket yang melintasi jaringan secara real time dan file logging ke dalam databasee. Snort merupakan salah satu contoh jenis IDS yang termasuk kategori network-based intrusion detection system (NIDS), yaitu sebuah program sistem yang dapat mendeteksi suatu (intrusion) penyusupan di dalam sistem jaringan komputer. Snort juga dapat bekerja sebagai mode packet sniffer yang memungkinkan sistem dapat membaca traffic jaringan komputer, dan Snort juga dapat bekerja dalam mode packet-loggeryang memugkinkan sistem mencatat traffic jaringan dan memberi peringatan yang terjadi. Snort suatu perangkat lunak untuk mendeteksi penyusup dan mampu dapat menganalisis lalu lintas real-time, hal ini dapat mendeteksi berbagai jenis serangan. Snort bukanlah sebatas protocol analisis atau sistem pendeteksi penyusupan (Intrusion Detection System) IDS, melainkan sedikit gabungan diantara

keduanya, dan bisa sangat berguna dalam merespons insiden-insiden peyerangan terhadap hosthost jaringan. Fitur Snort dapat menjadi penolong administrator sistem dan jaringan, dimana mampu memperingatkan kita atas penyusup yang berpeluang berbahaya.

Tabel 3.1 Perancangan Pendeteksi Serangan *IDS* dengan Menggunakan *Snort*

No	IP Adress	PORT	TTL
1.	192.168.59.128	8006	64
2.	192.168.59.128	39244	64
3	104.46.162.226	443	64
4	192.168.59.129	54878	64
5	192.168.59.129	50634	64
6	192.168.59.129	50012	64
7	20.190.154.136	443	64
8	192.168.59.129	53672	64
9	192.168.59.129	53382	64
10	192.168.59.129	39374	64
11	104.46.162.226	443	64
12	192.168.59.129	51656	64
13	91.189.91.38	80	128
14	192.168.59.129	51656	128
15	92.168.59.128	47818	64
16	91.189.91.38	80	64
17	192.168.59.129	47818	128
18	192.168.59.128	8006	64
19	192.168.59.129	39374	64
20	192.168.59.128	8006	128
21	192.168.59.1	57621	64
22	192.168.59.255	57621	128
23	192.168.59.128	57621	64
24	192.168.59.255	57621	128
25	192.168.59.129	51656	128
26	91.189.91.38	80	64
27	192.168.59.129	39374	64
28	192.168.59.128	8006	64
29	91.189.91.38	80	64
30	192.168.59.128	8006	64

3.1.2 Pengujian Server Cloud Computing

Hasil pengujian bertujuan untuk menunjukkan performansi server cloud computing yang telah dirancang apakah sudah berjalan dengan baik atau belum, karena dengan adanya hasil pengujian dapat memberikan informasi dalam keberhasilan penerapan sistem server cloud computing IPS melakukan proses monitoring dan tindakan berdasarkan aturan yang dibuat penggunanya. Sistem dapat melihat kegiatan yang ada di jaringan dengan mendeteksi aktivitas yang dilakukan pada pengguna jaringan. Client menyerang dengan memberikan sebuah permintaan yang besar ke server, paket akan melewati firewall bawaan server sebelum sistem mendeteksi paket. Penelitian ini paket yang menuju port icmp, tcp dan udp, menjadi fokus utama pengamanan serangan pada server. Paket yang telah dideteksi melewati jaringan akan disaring (filter) oleh aturan (rule).yang telah dibuat pengguna, data aktivitas jaringan akan di simpan untuk di tampilkan pada website. Memonitoring data serangan tersebut admin dapat memberi tindakan serangan berdasarkan IP Address penyerang, tindakan tersebut menggunakan fitur iptables melalui website. Pada penelitian ini Intrusion Prevention System (IPS) menggunakan snort sebagai sistem untuk memonitoring dan penyaringan data dan IPTables untuk melakukan tindakan dari serangan

Hasil dari pengujian yang sudah dilakukan ini dapat dilihat dalam tabel hasil pengujian sistem berikut ini :

Tabel 3.2 Hasil Pengujian *Server Cloud Computing*

No	Hak Akses *Client*	Port	Login	
			Berhasil	Gagal
1.	Kepala Sub bagian Keuangan, Perencanaan,evaluasi, dan Pelaporan.	8006	✓	-
2.	Kepala Sub Bagian Umum dan Kepegawaian	8006	✓	-
3.	Kepala Seksi Statistik	8006	✓	-
4.	Kepala Seksi layanan aplikasi	8006	✓	-
5.	Kepala Seksi Infrastruktur Teknologi dan persandian	8006	✓	-
6.	Kepala Seksi dokumentasi dan hubungan media	8006	✓	-
7.	Kepala Seksi pengelolaan informasi publik	8006	✓	-
8.	Kepala Seksi pengelolaan komunikasi publik	8006	✓	-

server cloud computing dengan hak akses client berhasil dan tidak dapat penyusup menyerang ip pada server cloud computing dengan metode intrusion detection system dapat melihat ip penyusup pada server cloud computing dengan ip dan port yang berbeda beda untuk menyerang cloud computing dan metode intrusion prevention system untuk memblokir ip yang telah dideteksi oleh intrusion detection system dan menutup ip dan port-port yang menyerang server cloud computing dan hasil pengujian ip penyusup tidak dapat mengakses server cloud computing.

Tabel 5.6 Data Kecepatan Bandwitch sebelum diterapkan *IDS* dan *IPS*

No	Nama	Sebelum diterapkan IDS & IPS (BPS)		Setelah diterapkan IDS & IPS (BPS)	
		Download	Upload	Download	Upload
1	Kepala Sub bagian Keuangan Perencanaan, evaluasi,dan Pelaporan.	7,99	9.42	Tidak Bisa Download	Tidak Bisa Upload
2	Kepala Sub Bagian Umum dan Kepegawaian	7.22	8.25	Error	Error
3	Kepala Seksi Statistik	5.22	6.72	Error	Error
4	Kepala Seksi layanan aplikasi	9.54	8.90	Error	Error
5	Kepala Seksi Infrastruktur Teknologi dan persandian	11.71	10.51	Error	Error

No	Nama	Sebelum diterapkan IDS & IPS (BPS)		Setelah diterapkan IDS & IPS (BPS)	
6	Kepala Seksi dokumentasi dan hubungan media	7.17	8.17	Eror	Eror
7	Kepala Seksi pengelolaan informasi public	3.90	4.32	Eror	Eror
8	Kepala Seksi pengelolaan komunikasi public	7.45	9.80	Eror	Eror
Rata-rata kecepatan		14.97	6.92	Eror	Eror

Pada tabel hak akses user dengan sebelum penerapan metode Intrusion Detection System dan Intrusion Prevention System, hak akses user mendapatkan kecepatan download rata-rata 15.97 dan upload dengan kecepatan 6.92 dan setelah diterapkannya metode Intrusion Detection System dan Intrusion Prevention System dari hak akses yang tadi dapat bisa mengakses kecepatan bandwitchnya sekarang menjadi error atau tidak dapat mengakses server dan tidak dapat mendapatkan kecepatan bandwitch dan semua tampilan server cloud storage tidak dapat menampilkan struktural dan user sebagai pegawai dinas komunikasi dan informatika kota Padang Panjang.

2. METODE PENELITIAN

Metodologi penelitian ini menjelaskan beberapa aturan dan prosedur yang akan dilakukan untuk dapat menyelesaikan permasalahan yang akan terjadi pada objek sehingga diadakan penelitian diharapkan dapat memberikan solusi yang bermanfaat tehadapat permasalahan tersebut. Metode penelitian ini merupakan teknik-teknik yang dipakai dalam merumuskan, menganalisa, mengumpulkan data sampai dengan proses implementasi hasil penelitian.

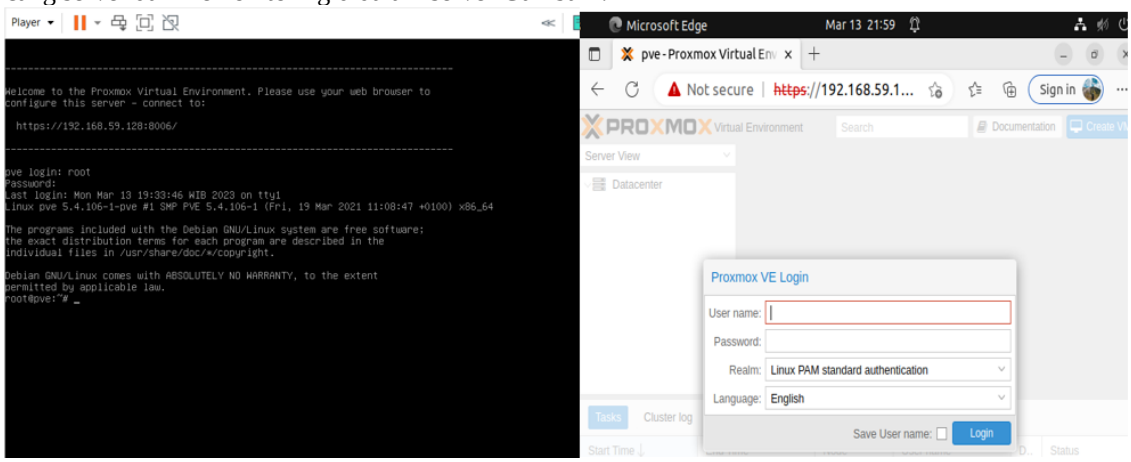
Metode penelitian Tujuan dari penelitian ini adalah mengaplikasikan Cloud Computing dengan metode Intrusion Detection System dan Intrusion Prevention Sytem dalam mengoptimalkan penggunaan Cloud Storage terhadap pelayanan koneksi jaringan internet pada Diskominfo Kota Padang Panjang, rangkaian kegiatan ilmiah ini disusun dalam sebuah kerangka kerja yang akan dijelaskan pada pembahasan di bawah.

3. HASIL IMPLEMENTASI

Merupakan tahapan meletakkan sistem supaya siap untuk dioperasikan dan dapat dipandang sebagai usaha untuk mewujudkan sistem yang telah dirancang langkah – langkah dalam tahap implementasi ini adalah urutan kegiatan awal samapai akhir yang harus dilakukan dalam mewujudkan sistem yang telah di rancang yaitu:

1. Proses Login Admin Proxmox

Pada tampilan perancangan proxmox ve terdapat tampilan untuk login pada proxmox dan setelah login masuk ke browser agar dapat login diusername dan password dan tampilan server cloud storage dapat merancang server dan memonitoring didalam server Gambar1.1

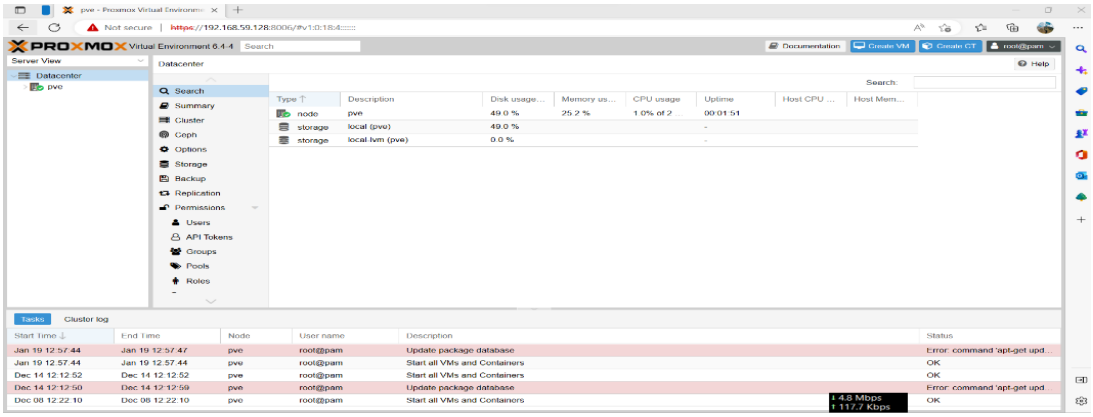


Gambar 4.1 Tampilan *Perancangan Proxmox*

Setelah admin memasukkan *username* dan *password valid*, maka *admin* dapat menggunakan sistem ini dan dihadapkan pada halaman menu utama.

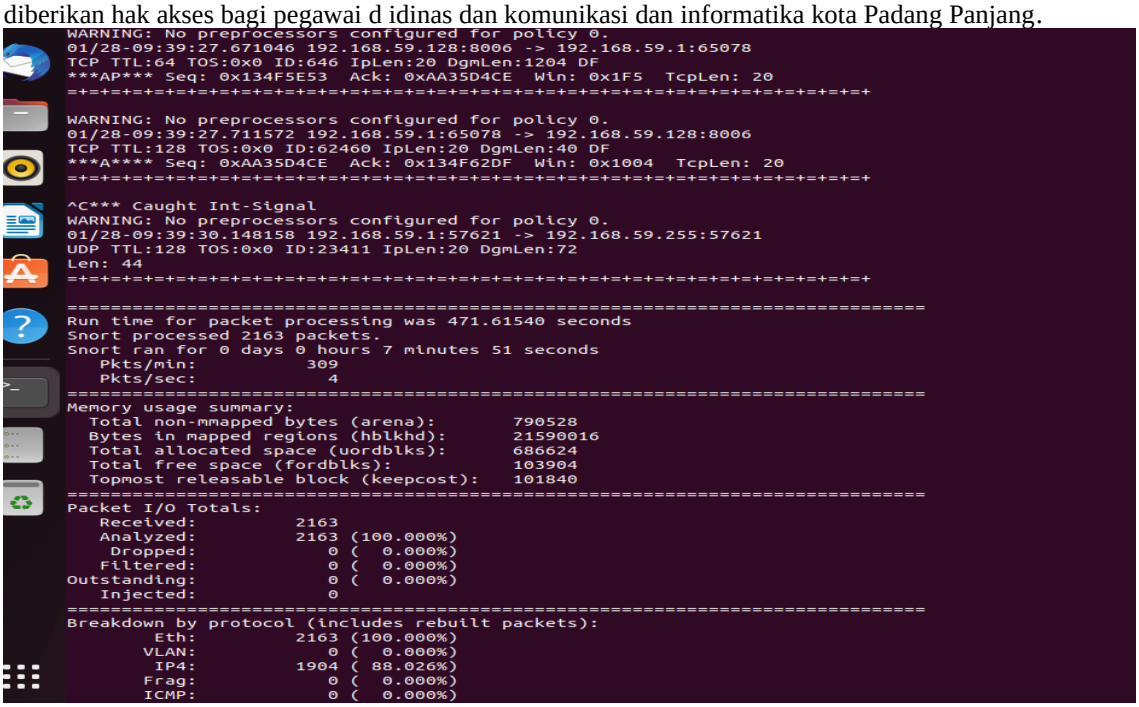
2. Implementasi Dengan Proxmox VE

Tampilan Proxmox VE merupakan sistem operasi mesin virtual yang mulai banyak dipakai oleh para pengguna teknologi virtualisasi. ProxmoxVE juga dilengkapi dengan alat bantu command line dan REST API untuk alat bantu pihak ketiga. Keunggulan Proxmox VE antara lain High Availability Cluster, Live Migration, bridged networking, flexible storage, OS template building, scheduled backup, dan command line tools Gambar 5.1 berikut :



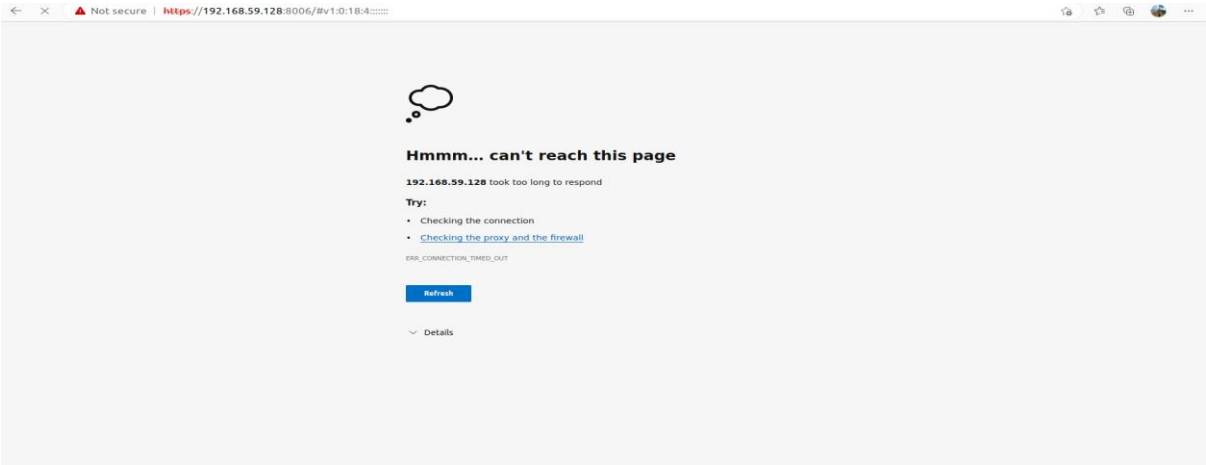
Gambar 4.2 Tampilan awal Proxmox pada Browser

Dari gambar diatas menunjukan Hak akses stuktural dalam grup adalah kepala bidang dari User yang telah diberikan hak akses bagi pegawai d idinas dan komunikasi dan informatika kota Padang Panjang.



Gambar 4.3 Tampilan Port Scanning

Tampilan Gambar 5.3 terdapat ip yang terdeteksi oleh port scanning dengan ip dan port port yang terbuka dengan melihat ip cloud storage 192.168.59.128 dan setelah discaning dan TTL yang berbeda beda dan TTl yang muncul 128 dan 64 paling banyak yang merespon ip cloud storage.



Gambar 4.4 Hasil Pengujian Dengan Menggunakan Metode IDS dan IPS

KESIMPULAN

Berdasarkan hasil penelitian dan pembahasan yang telah dilakukan tentang metode Intrsuion Detection System dan Intrusion Prevention System, dapat diambil kesimpulan yaitu:

1. Virtualisasi menggunakan Proxmox VE dapat dilakukan secara virtual dengan menggunakan VMware Workstation 16 sebagai prompt console nya dan dikonfigurasi di browser sebagai cloud server nya. Dengan menggunakan proxmox yang dapat meminimalisir maintenance dan anggaran untuk pengadaan hardware. Layanan penyimpanan (storage) hanya bisa diakses dengan menjalankan Virtual machine yang terdapat pada server dan dikonfigurasikan menjadi sebuah storage untuk di share dengan sesama pengguna layanan cloud computing. Server ini juga dapat dibangun dalam bentuk virtualisasi dengan model private cloud storage sehingga untuk mengakses server membutuhkan akses jaringan LAN (Local Area Network).
2. Metode IDS merupakan suatu perangkat lunak untuk mendeteksi penyusup dan mampu dapat menganalisis lalu lintas real-time, hal ini dapat mendeteksi berbagai jenis serangan masuk. Fitur Snort juga dapat menjadi penolong administrator pada sistem dan jaringan, dimana mampu memperingatkan kita atas penyusup yang berpeluang berbahaya mengancam sebuah keamanan. Metode IPS mampu mencegah serangan port scanning yang dilakukan oleh attacker terhadap server cloud computing dengan cara mengaktifkan fitur firewall dan mengkonfigurasikannya dengan iptables dan IPS bertindak seperti layaknya firewall yang akan mengizinkan atau menghalang paket data Secara khusus kepada komponen yaitu Normalisasi Traffic,Detection Engine,Service Scanner,Traffic Shaper. IPS mengombinasikan teknik firewall dan metode intrusion detection system (IDS) dengan sangat baik. Teknologi ini dapat digunakan untuk mencegah serangan yang akan masuk ke jaringan lokal dengan memeriksa dan mencatat semua paket data serta mengenali paket dengan sensor saat seragan teridentifikasi.

Saran

Adapun beberapa saran yang perlu dikaji dari pengembangan sistem pendukung keputusan ini yaitu:

1. Pengembangan lebih lanjut, sebaiknya server yang digunakan menggunakan perangkat komputer dengan spesifikasi yang tinggi dan kapasitas server yang baik. Dan penerapannya dilakukan pada hard drive bukan secara virtual demi meningkatkan performansi penggunaan cloud storage pada Dinas Komunikasi dan Informatika Kota padang Panjang.
2. Aspek pemeliharaan server secara berkala sangat perlu dilakukan agar server yang bersifat virtualisasi tersebut dapat bertahan dalam waktu yang lama. Dan dapat mengembangkan layanan Software yang dapat menyediakan aplikasi maupun software yang dapat diakses via internet dan digunakan secara bersamaan oleh seluruh pengguna internet dan menambah dan menerapkan layanan yang lain.

DAFTAR PUSTAKA

[1] S. Al-Ridwan Iqbaal, A. Maulana, and N. Sulistiyowati, "Analisis Quality Of Service (QOS) Pada Jaringan Internet Yayasan Rumah," *J. Ilm. Wahana Pendidik.*, vol. 8, no. 16, pp. 276–280, 2022, [Online]. Available: https://doi.org/10.5281/zenodo.7067627

[2] Wawan Setiawan, Nurul Fajriyah, and Tobias Duha, "Analisa Layanan Cloud Computing Di Era

Digital," *J. Inform.*, vol. 1, no. 1, 2022.
[3] D. Satrinia, S. N. Yutia, and I. M. M. Matin, "Analisis Keamanan dan Kenyamanan pada Cloud Computing Dwina Satrinia #1 , Syifa Nurgaida Yutia #2 , Iik Muhamad Malik Matin #3," *J. Informatics Commun. Technol.*, vol. 4, no. 1, pp. 85–91, 2022.
[4] E. Prasetyo, J. Dedy Irawan, and F. X. Ariwibisono, "Rancang Bangun Sistem Monitoring Server Virtual Berbasis Web Menggunakan Script Monitoring Pada Proxmox Virtual Environment," *JATI (Jurnal Mhs. Tek. Inform.*, vol. 6, no. 1, pp. 179–185, 2022, doi: 10.36040/jati.v6i1.4550.
[5] D. Diana, I. Seprina, and S. O. Kunang, "Pelatihan Manajemen Penyimpanan Online (Cloud Storage) pada Guru SMP Al-Hamidiyah Palembang," *J. Pengabdi. Pada …*, vol. 6, no. 4, pp. 1259–1267, 2021, doi: 10.30653/002.202164.841.
[6] S. Khadafi, Y. D. Pratiwi, and E. Alfianto, "Keamanan Ftp Server Berbasiskan Ids Dan Ips Menggunakan Sistem Operasi Linux Ubuntu," *Netw. Eng. Res. Oper.*, vol. 6, no. 1, p. 11, 2021, doi: 10.21107/nero.v6i1.190.
[7] F. Tanang Anugrah, S. Ikhwan, and J. Gusti A.G, "Implementasi Intrusion Prevention System (IPS) Menggunakan Suricata Untuk Serangan SQL Injection," *Techné J. Ilm. Elektrotek.*, vol. 21, no. 2, pp. 199–210, 2022, doi: 10.31358/techne.v21i2.320.
[8] M. Fadhlurrohman, A. Muliawati, and B. Hananto, "Analisis Kinerja Intrusion Detection System pada Deteksi Anomali dengan Metode Decision Tree Terhadap Serangan Siber Analysis of Intrusion Detection System Performance on Anomaly Detection with Decision Tree Method Against Cyber Attacks," *J. Ilmu Komput. Agri-Informatika*, vol. 8, no. Pratomo 2016, pp. 90–94, 2021.
[9] T. Widodo and A. S. Aji, "Pemanfaatan Network Forensic Investigation Framework untuk Mengidentifikasi Serangan Jaringan Melalui Intrusion Detection System (IDS)," *JISKA (Jurnal Inform. Sunan Kalijaga)*, vol. 7, no. 1, pp. 46–55, 2022, doi: 10.14421/jiska.2022.7.1.46-55.
[10] R. Susanto, "Rancang Bangun Jaringan Vlan dengan Menggunakan Simulasi Cisco Packet Tracer," *J. Nas. Inform. dan Teknol. Jar.*, vol. 4, no. 2, pp. 1–6, 2020.
[11] Z. Munawar, M. Kom, and N. I. Putri, "Keamanan Jaringan Komputer Pada Era Big Data," *J. Sist. Informasi-J-SIKA*, vol. 02, pp. 14–20, 2020.
[12] D. Santoso, A. Noertjahyana, and J. Andjarwirawan, "Implementasi dan Analisa Snort dan Suricata Sebagai IDS dan IPS Untuk Mencegah Serangan DOS dan DDOS," *J. Infra*, vol. 10, no. 1, pp. 1–6, 2022, [Online]. Available: https://publication.petra.ac.id/index.php/teknik-informatika/article/view/12033
[13] Muh. Miftakhun Nizar, R. Alit, and F. Prima Aditiawan, "Implementasi Metode Moora Pada Sistem Pendukung Keputusan Pemilihan Smartwatch Terbaik," *J. Inform. dan Sist. Inf.*, vol. 2, no. 1, pp. 34–42, 2021, doi: 10.33005/jifosi.v2i1.269.
[14] R. Nindyasari, A. C. Murti, and M. I. Ghozali, "ANALISIS QoS (Quality of Service) JARINGAN UNBK DENGAN MENGGUNAKAN MICROTIC ROUTER (Studi Kasus : Jaringan UNBK SMAN 1 Jakenan Pati)," *Netw. Eng. Res. Oper.*, vol. 4, no. 2, pp. 109–116, 2019, doi: 10.21107/nero.v4i2.126.