

**PERANCANGAN KEAMANAN JARINGAN KOMPUTER PADA LAYER  
APPLICATION BERBASIS INTRUSION PREVENTION SYSTEM (IPS) YANG DI  
INTEGRASIKAN DENGAN ACCESS CONTROL LIST (ACLs)**

**COMPUTER NETWORK DESIGN SECURITY IN LAYER APPLICATION BASED  
ON INTRUSION PREVENTION SYSTEM (IPS) INTEGRATED WITH ACCESS  
CONTROL LIST (ACLs)**

**Dahlan**

**Arief Zulianto**

Program Studi Teknik Informatika  
Program Pascasarjana Universitas Langlangbuana  
jurnalpascaunla@gmail.com

---

**ABSTRAK**

Jaringan Komputer yang ada di Politeknik TEDC antar departemen satu dengan departemen yang lain saling terhubung dalam jaringan Lokal Area Network, untuk membagi segmentasi jaringan berdasar pada fungsi, project team, atau aplikasi organisasi dengan mengabaikan penempatan fisik atau koneksi ke jaringan, oleh karena itu perlu di buat *workgroup* sesuai dengan departemen. User yang terhubung dalam jaringan tersebut tentunya berkesempatan untuk mengakses ke sumber daya padahal sebagian user tidak diperbolehkan karena tidak mempunyai kepentingan terhadap sumber daya tersebut. Untuk menseleksi user yang boleh akses (*permit*) atau di tolak (*deny*) pada akses ke sumber daya tentunya di perlukan penanganan lebih selektif terhadap permintaan user. Begitu juga dalam melakukan pencegahan dini terhadap penyusup yang dapat merusak sebuah *system* maka di perlukan penanganan, agar *system* jaringan akan selalu terjaga dari penyusup dan aplikasi-aplikasi yang mencurigakan. Untuk melakukan pembagian segmentasi jaringan di Politeknik TEDC di buat *Virtual Local Area Network (VLAN)* yang secara logika membagi jaringan ke dalam *broadcast domain* berbeda sehingga paket *switch* antara port yang ditunjuk untuk VLAN yang sama. VLAN diciptakan untuk menyediakan layanan segmentasi biasa yang diberikan oleh router fisik dalam konfigurasi LAN. Router pada topologi VLAN menyediakan penyaringan broadcast, keamanan, mengatur alur lalu lintas dan mengatur otorisasi terhadap user dengan menerapkan konsep *Access Control List (ACLs)* yang dapat di konfigurasi pada router. Sedangkan *Intrusion Prevention System (IPS)* yang di terapkan pada Server dengan menggunakan *Snort* sebagai *tools* nya dan *Acid-MySQL* sebagai *Database* *Snort*, bertujuan untuk mencegah jika adanya penyusup atau aplikasi yang mencurigakan. Sehingga dengan adanya perancangan keamanan jaringan komputer yang berbasis *Intrusion Prevention System* dan dengan *Access Control List (ACLs)* yang di terapkan di Politeknik TEDC di harapkan dapat mengamankan jaringan komputer dengan mendeteksi secara dini jika adanya *intruder* yang akan merusak pada sistem jaringan dan juga dapat mengatur otorisasi terhadap user yang mengakses sumber daya dalam segmentasi jaringan.

**Kata kunci :** VLAN, ACLs, IPS, Snort, Acid-MySQL, Keamanan Jaringan,

**ABSTRACT**

*Computer Networks in the TEDC Polytechnic between departments one with interconnected departments within the Local Area Network , to divide network segmentation based on*

function, project team, or organizational application with physical access or connection to the network, therefore need to make workgroup appropriate with the department. Users who are connected in the network of course the opportunity to access to the resources of some users are not allowed because it has no interest in those resources. To select users who may have access (permission) or deny access to resources of course need more selective handling of user requests. So also in doing early prevention of intruders that can damage a system then in need awake, so that the system will always be awake from the intruder and suspicious applications. To divide network segmentation at TEDC Polytechnic, create a Virtual Local Area Network (VLAN) that logically connects into different broadcast domains with switch packets between ports designated for the same VLAN. VLANs are created to provide the usual segmentation services provided by physical routers in LAN configuration. Routers in VLAN topologies provide broadcast filtering, security, workflow manage and access. Access Control Lists (ACLs) that can be configured on the router. While the Intrusion Prevention System (IPS) is applied to the Server by using Snort as its tool and Acid-MySQL as the Snort Database, the option to prevent any intruders or suspicious applications. With the design of network security based on Intrusion Prevention System and with Access Control List (ACLs) which applied in TEDC Polytechnic in can computer network with early if there is intruder that will damage on network system and also can arrange authorization to user access in network segmentation.

**Keywords:** VLAN, ACL, IPS, Snort, Asam-MySQL, Network Security,

## 1. PENDAHULUAN

Jaringan komputer bukanlah sesuatu yang baru saat ini. Hampir di setiap perusahaan/institusi termasuk di Politeknik TEDC Bandung terdapat jaringan komputer, Di Politeknik TEDC Bandung seluruh departemen terhubung dalam satu jaringan Lokal Area yang dapat mengakses sumber daya baik lewat jaringan lokal maupun Internet. Tidak adanya pemisah segmentasi menimbulkan sulitnya melakukan pengontrolan terhadap seluruh user.

Protocol Application Layer digunakan untuk pertukaran data antara program yang berjalan pada source dan host tujuan. Dengan kata lain, application layer berfungsi sebagai antarmuka dengan aplikasi dengan fungsionalitas jaringan, mengatur bagaimana aplikasi dapat mengakses dalam sebuah jaringan, tentunya perlu dilakukan pengamanan.

Untuk mempermudah pengontrolan user agar sesuai dengan fungsinya, maka di Politeknik TEDC Bandung perlu di buat segmentasi dengan menerapkan

access control list sebagai pengatur hak akses dan intrusion prevention system merupakan system pengamanan terhadap aplikasi-aplikasi yang mencurigakan yang dilakukan melalui application layer.

## 2. METODE PENELITIAN

Action research menurut Davison, Martinson dan Knock (2004) yaitu penelitian tindakan yang mendeskripsikan, menginterpretasi dan menjelaskan suatu situasi sosial atau pada waktu bersama dengan melakukan perubahan atau intervensi dengan tujuan perbaikan atau partisipasi. Adapun tahapan penelitian yang merupakan bagian dari action research ini, yaitu :

### a. Tahap pertama (Diagnosing)

Melakukan identifikasi masalah-masalah pokok yang ada, guna menjadi dasar kelompok atau organisasi sehingga terjadi perubahan. Peneliti melakukan diagnosa terhadap infrastruktur jaringan komputer di Politeknik TEDC Bandung

b. **Tahap kedua(Action Planning)**

Peneliti memahami pokok masalah yang ada kemudian dilanjutkan dengan menyusun rencana tindakan yang tepat. Pada tahap ini peneliti melakukan rencana tindakan yang akan dilakukan pada jaringan dengan membuat Perancangan Perancangan Keamanan Jaringan Komputer Pada Layer Application Berbasis Intrusion Prevention System (IPS) Yang di Integrasikan Dengan Access Control List (ACLs) di Politeknik TEDC .

c. **Tahap ketiga(Action Taking)**

Peneliti melakukan tindakan disertai dengan implementasi rencana yang telah dibuat dan mengamati kinerja Perancangan Keamanan Jaringan Komputer Pada Layer Application Berbasis Intrusion Prevention System (IPS) Yang di Integrasikan Dengan Access Control List (ACLs) di Politeknik TEDC.

d. **Tahap keempat(Evaluating)**

Peneliti melakukan evaluasi hasil temuan setelah proses implementasi, pada tahap evaluasi penelitian yang dilakukan adalah hasil implementasi Perancangan Keamanan Jaringan Komputer Pada Layer Application Berbasis Intrusion

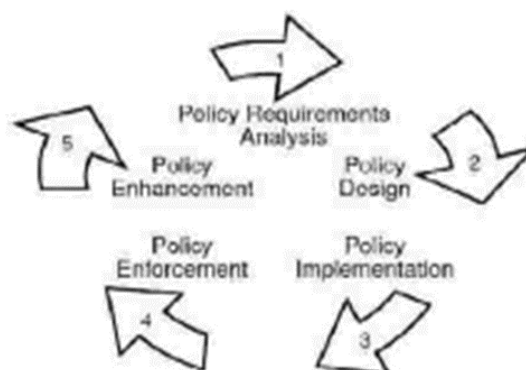
Prevention System (IPS) Yang di Integrasikan Dengan Access Control List (ACLs) di Politeknik TEDC.

e. **Tahap kelima(Learning)**

Setelah masa implementasi (*action research*) dianggap cukup, kemudian peneliti melaksanakan *review* tahap demi tahap dan memahami prinsip kinerja Keamanan Jaringan Komputer Pada Layer Application Berbasis Intrusion Prevention System (IPS) Yang di Integrasikan Dengan Access Control List (ACLs) di Politeknik TEDC.

### 3. METODE PENGEMBANGAN SYSTEM

*Security Policy Development Life Cycle* (SPDLC) adalah suatu pendekatan proses dalam komunikasi data yang menggambarkan siklus yang tindakan awal dan akhirnya dalam membangun sebuah keamanan jaringan komputer mencakup lima tahap yaitu *Analysis, Design, Implementation, Enforcement, dan Enhancement* (Wahsheh dan Jim, 2008: 1121).



Gambar 2.15 Security Policy Development Life Cycle (SPDLC)

(Sumber Luay A. Wahsheh and Jim Alves-Foss, 2008:1121)

## 1. Analysis

Pada tahap ini dilakukan perumusan masalah, mengidentifikasi konsep dari IPS, ACLs dan beberapa perangkat jaringan, mengumpulkan data dan mengidentifikasi kebutuhan seluruh komponen sistem tersebut, sehingga spesifikasi kebutuhan sistem keamanan jaringan komputer pada layer Application dengan metode IPS dan ACLs dapat diperjelas dan terperinci.

## 2. Design

Pada tahap ini yang dilakukan adalah Merancang topologi jaringan untuk simulasi *Virtual Local Area Network* sebagai representasi lingkungan jaringan sebenarnya dan merancang penggunaan sistem operasi dan aplikasi pada server, client dan komputer penyusup. Rancangan topologi jaringan dibangun dengan menggunakan Cisco Packet Tracer 5.0 yang sudah terinstal.

## 3. Implementation

Implementasi atau penerapan detail rancangan topologi dan rancangan sistem pada lingkungan nyata sebagai simulasi *Virtual Local Area Network*. Detail rancangan akan digunakan dapat dilihat sebagai intruksi atau panduan tahap implementasi agar sistem yang dibangun dapat relevan dengan sistem yang sudah dirancang. Proses implementasi terdiri dari instalasi dan konfigurasi. Dengan mengumpulkan seluruh perangkat yang dibutuhkan.

## 4. Enforcement

Dimana tahap ini penting. Proses pelaksanaan atau penyelenggaraan dilakukan melalui aktivitas pengoperasian dan pengamatan sistem yang sudah dibangun dan diterapkan apakah sistem

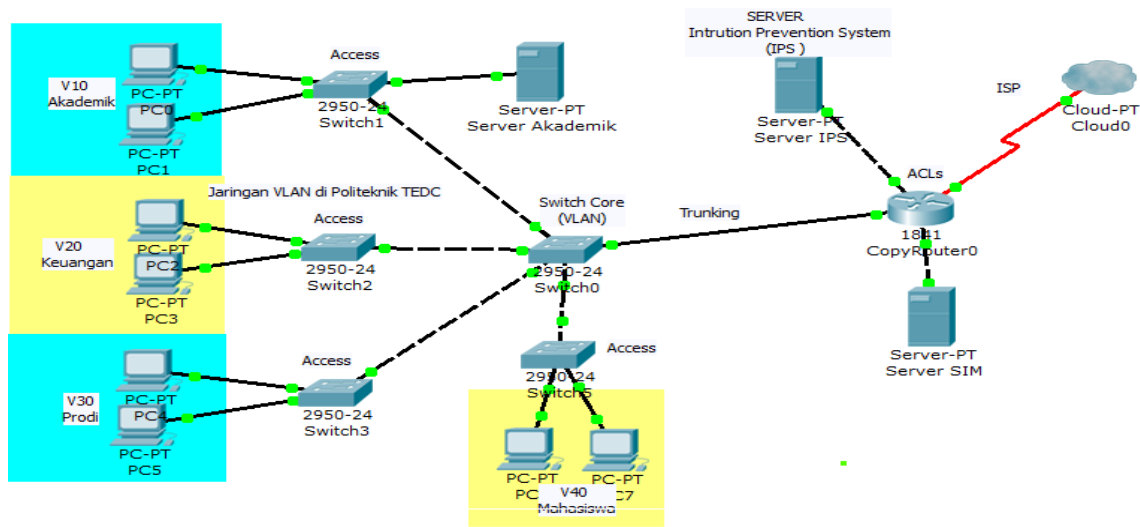
IPS, Access Control List dan Pembagian Segmentasi jaringan sudah berjalan dengan benar dan baik.

## 5. Enhancement

Pada fase atau tahap ini dilakukan aktivitas perbaikan terhadap perancangan dan sistem yang telah dibangun

## 4. HASIL DAN PEMBAHASAN

Pada tahap ini penulis mendefinisikan bahwa jaringan yang ada di Politeknik TEDC semua departemen, seperti bagian Keuangan, Akademik, Prodi, Mahasiswa dan Dosen semua terhubung dalam jaringan LAN, yang tentunya terhubung dalam jaringan lokal area network dalam satu segmentasi. Tahapan dalam pembagian segmentasi jaringan guna mempermudah pengontrolan hak akses atau penerapan ACLs, sehingga terbentuk workgroup yang lebih mudah dalam pengontrolan user terhadap akses Sumber Daya. Dan Pengoperasian dan UjiCoba Pada tahap ini dilakukan uji coba (*testing*) terhadap konfigurasi Keamanan Jaringan pada Application Layer berbasis IPS yang diintegrasikan dengan ACLs yang telah didapat dari proses sebelumnya. Uji coba yang dilakukan dengan metode *enforcement*. Pengujian dilakukan dengan melakukan: Pengujian *host scanning* (angry ipscan), Pengujian *port scanning* (zenmap), Pengujian *HTTP attacking*, Pengujian *SSH* dan Pengujian *ping of death* serta Gambar topologi di bawah ini adalah rancangan yang akan di bangun untuk perancangan keamanan jaringan pada *apllication layer* berbasis *intrusion prevention system* yang diintegrasikan dengan *access control list*



Tabel untuk pembuatan segmentasi jaringan

| No | VLAN ID | Nama Vlan | Port   |
|----|---------|-----------|--------|
| 1  | 10      | AKADEMIK  | 3-8    |
| 2  | 20      | PRODI     | 9- 14  |
| 3  | 30      | KEUANGAN  | 15-20  |
| 4  | 40      | KESISWAAN | 21 -24 |

Tabel Pembagian IP addressing

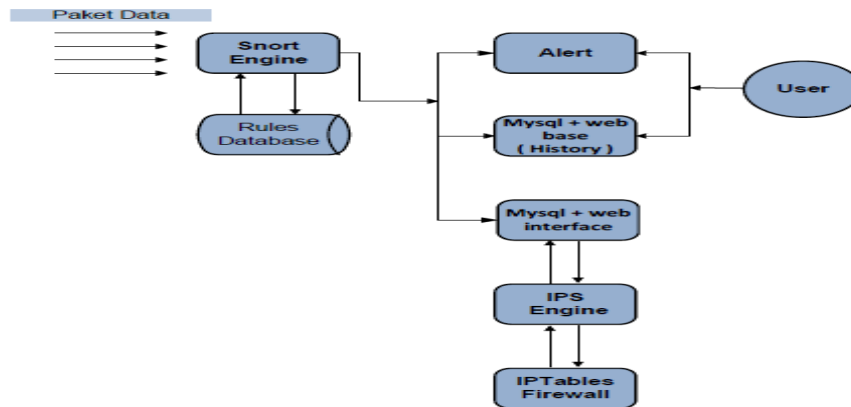
| No | VLAN ID | Nama Vlan          | Type   |
|----|---------|--------------------|--------|
| 1  | 10      | 192.168.1.0 /26    | DHCP   |
| 2  | 20      | 192.168.1.64 /27   | DHCP   |
| 3  | 30      | 192.168.1.96 /27   | DHCP   |
| 4  | 40      | 192.168.1.128 /28  | DHCP   |
| 5  | SERVER1 | 192.168.11.100 /24 | STATIC |
| 6  | SERVER2 | 192.168.100.100/24 | STATIC |

Tabel Komponen Perancangan IPS, ACLs dan VLAN

| Mesin                       | Komponen                                                                                                                                                                                          | Keterangan                                                                                                                                                                                                                                         |
|-----------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Router Cisco                | -                                                                                                                                                                                                 | Digunakan dalam konfigurasi untuk mengatur trafik dan otorisasi pada penerapan Access Control List                                                                                                                                                 |
| Switch Ciso Manageble       |                                                                                                                                                                                                   | Digunakan dalam konfigurasi untuk membagi segmentasi jaringan                                                                                                                                                                                      |
| Sensor IPS                  | 1. IDS <ul style="list-style-type: none"> <li>a. Snort Engine</li> <li>b. Rule Snort</li> </ul> 2. Data Base System           3. IPS Engine           4. IP Tables           5. Monitoring System | Sensor ini digunakan untuk mengintegrasikan fungsi menganalisis traffic sebuah sistem jaringan dan mendeteksi aktivitas intruder (Snort), Pengelola Output Snortsam, Management console dan alert dari Snort, dan IP Table sebagai <i>Firewall</i> |
| Client Linux Backtrack 4 R2 | 1. Backtrack tools                                                                                                                                                                                | Mendefinisikan sebagai client dan juga untuk pengujian sistem sensor                                                                                                                                                                               |

Sistem keamanan ini bertujuan untuk mencegah dan melindungi jaringan *layer Application* dengan kemampuan merespon serta aksi terhadap suatu intrusi

sesuai dengan kebijakan keamanan. Untuk lebih jelas seperti gambarkan sebagai berikut:



Gambar 4.4 : Hubungan Antara Sensor Snort  
(Sumber : Gullett, David : 2011)

Dari diagram pada gambar 4.4 IPS yang akan dipakai merupakan integrasi dari beberapa aplikasi *open source* dimana ada beberapa modul yang akan digunakan didalamnya diantaranya sebagai berikut :

#### 1. Snort Engine

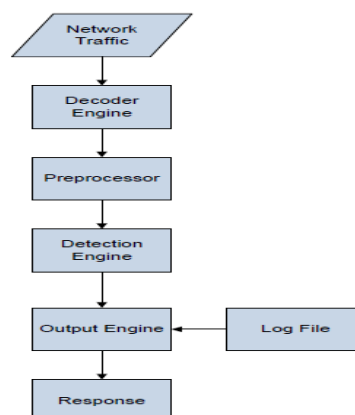
Snort Engine merupakan program yang selalu bekerja untuk membaca paket data dan kemudian membandingkan dengan *rule* Snort.

```

root@myubuntu:~# ps aux | grep snort
snort  2656 0.1 1.9 58376 38164 ?        Ss   23:08   0:00 /usr/sbin/snort -m
027 -D -d -l /var/log/snort -u snort -g snort -c /etc/snort/snort.conf -S
HOME_NET=[192.168.1.0/24] -i eth0
root   2847 0.0 0.0 3324  812 pts/0    S+   23:12   0:00 grep --color=auto
  
```

Perintah diatas menunjukkan bahwa Snort Engine dalam keadaan aktif dengan proses ID 2847 dan dijalankan oleh user

“root”. Cara kerja *snort* akan digambarkan pada *flowchart* berikut



Gambar 4.5: Flowchart Snort Engine (Sumber : Gullett, David : 2011)

#### 2. Rule Snort

Rule Snort merupakan *database* yang berisi pola-pola serangan berupa

signature jenis-jenis serangan. Contoh

rule Snort:

```
alert tcp $EXTERNAL_NET any <> $HOME_NET 0 (msg:"BAD-TRAFFIC
tcp port 0 traffic"; flow:stateless; classtype:misc-activity; sid:524; rev:8;)
alert udp $EXTERNAL_NET any <> $HOME_NET 0 (msg:"BAD-TRAFFIC
udp port 0 traffic"; reference:bugtraq,576; reference:cve,1999-0675;
reference:nessus,10074;
```

Rule diatas terdiri dari 2 bagian yaitu :header dan option. Bagian “alert tcp\$EXTERNAL\_NET any <> \$HOME\_NET 0” dan “alert udp \$EXTERNAL\_NET any <> \$HOME\_NET 0” adalah header dan selebihnyamerupakan bagian dari option. Dari rule Snort ini akan dikelompokkanapakah sebuah paket data

yang lewat dianggap sebagai sebuah serangan penyusupan atau bukan.

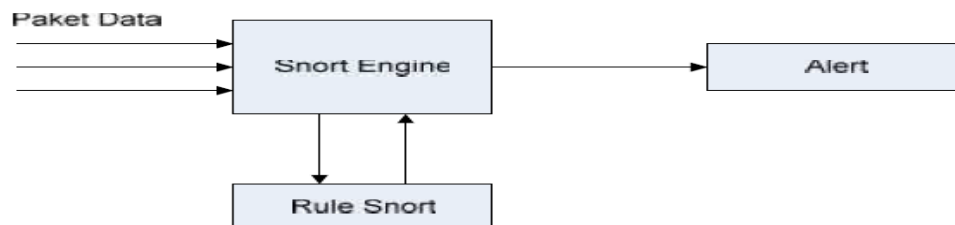
### 3. Alert

Alert merupakan catatan serangan pada deteksi serangan penyusupan. Jika rule Snort mendefinisikan paket data yang lewat sebagai serangan penyusupan, maka Snort Engine akan mengirimkan alert berupa log ke dalam database.

```
06/13-12:45:56.208898 *** [122:1:0] (portscan) TCP Portscan *** [Priority:
3] {PROTO:255} 192.168.1.246 => 192.168.1.244
06/13-12:45:56.208897 *** [122:1:0] (portscan) TCP Portscan *** [Priority:
3] {PROTO:255} 192.168.1.246 => 192.168.1.244
```

Contoh diatas merupakan alert hasil scanning port TCP dari IP192.168.1.246 ke IP 192.168.1.244 yang disimpan oleh Snort Engine ke dalam alert dan dianggap

sebagai sebuah serangan oleh Snort karena pola paket data tersebut terdapat dalam rule Snort. Hubungan ketiga komponen IDS dijelaskan dalam gambar berikut:

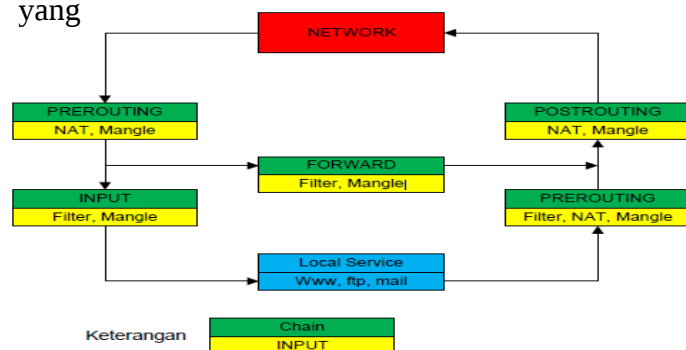


Gambar 4.6: Komponen Alert Snort  
(Sumber : Gullett, David : 2011)

### 4. IP Table

Firewall digunakan untuk membuka dan menutup akses sesuaidengan rule yang dibuat, dalam hal ini rule akan dinamis sesuaidengan kondisi yang

dideteksi oleh IDS. Firewall yangdigunakan dalam eksperimen ini adalah Iptables yangmerupakan firewall bawaan Linux



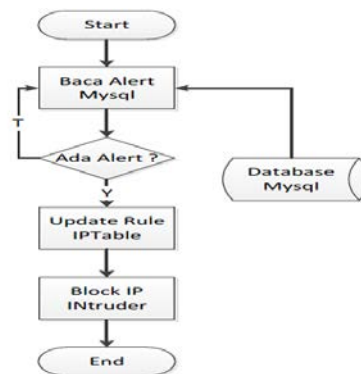
Gambar 4.7 Skema Filterisasi

(Sumber : Gullett, David : 2011)

IPS engine merupakan sistem yang akan membaca alertkemudian memerintahkan

firewall untuk menutup akses paket data dari penyerang. Cara kerja IPS engine

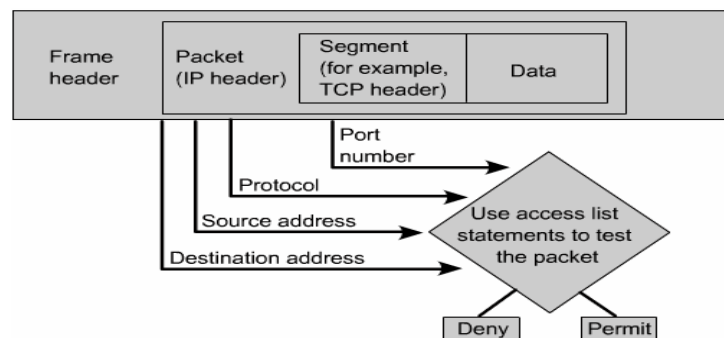
digambarkan dalam flowchart berikut ini:



Gambar 4.8 : Flowchar IPS Engine  
(Sumber : Gullett, David : 2011)

Sedangkan dalam menentukan hak akses apakah user boleh mengakses sumber daya atau sebaliknya maka dilakukan

konfigurasi pada router dengan Access Control List (ACLs) bisa di lihat pada gambar di bawah ini :



Gambar 4.12 : Cara kerja Access Control List  
(Sumber : CCNA, Todd Lammle : 2007)

### A. Pengujian Host Scanning

Pada pengujian ini dilakukan percobaan pengamatan terhadap host yang ada pada jaringan. Berikut contoh

pengujian serangan yang dilakukan menggunakan aplikasi Angry IPScan.

1. Kondisi Snort Network Intrusion Prevention System tidak aktif







## F. Pengujian Ping of Death

Pada pengujian ini, penyerang akan melakukan *Denial of Service* (DoS) berupa *Ping of Death*, yaitu

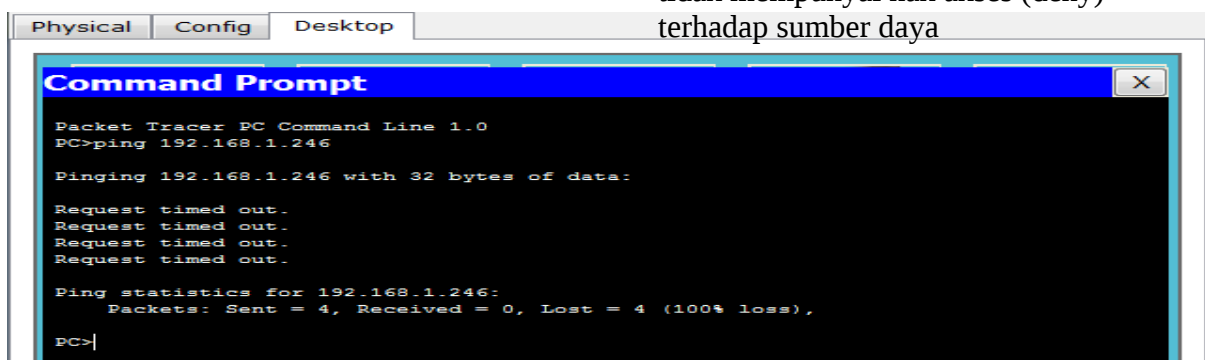
dengan mengirimkan paket ICMP dalam jumlah besar ke server NIPS.

1. Kondisi Snort Network Intrusion Prevention System tidak aktif



## G. Pengujian Access Control List (ACLs)

1. Pengujian dilakukan pada user yang tidak mempunyai hak akses (deny) terhadap sumber daya



## 5. KESIMPULAN

1. Dengan adanya pemisahan segmentasi jaringan, seluruh departemen yang ada di politeknik TEDC lebih mudah dalam pengontrolan, pengaturan hak akses dan

terpisah dalam sebuah workgroup. Sehingga departemen satu dengan yang lainnya tidak dapat mengintervensi dalam segmentasi yang berbeda.

2. Snort Network Intrusion Prevention System (NIPS) mampu monitoring

aktivitas dalam jaringan dan melakukan pencegahan secara dini apabila ada penyusup dan aplikasi-aplikasi yang mencurigakan, sehingga keamanan jaringan di Politeknik TEDC akan lebih aman dari user yang akan melakukan *intruder* terhadap sumber daya.

3. Keamanan jaringan merupakan aspek yang harus di perhatikan, di Politeknik TEDC semua user terhubung dalam satu jaringan, sehingga sangat sulit bagi admin jaringan dalam melakukan pengontrolan, monitoring, mengatur hak akses, dengan adanya penerapan keamanan jaringan yang berbasis IPS yang di Integrasiakan dengan ACLs di harapkan user bekerja sesuai dengan tugas dan tanggungjawabnya, jaringan komputer akan lebih aman dan nyaman, sehingga pelayanan terhadap kebutuhan informasi akan selalu tersedia.

## 6. DAFTAR PUSTAKA

- Alder, Raven. *Snort 2.1 Intrusion Detection, Second Edition*. Rockland, MA  
02370: Syngress Publishing, Inc. 2004  
. *Snort IDS and IPS Toolkit*. Burlington, MA 01803: Syngre Publishing, Inc. 2007
- Ariyus, D. 2007. *Intrusion Detection System*. Andi Yogyakarta. Yogyakarta.
- Arief M Rudianto. 2011. *Pemrograman Web Dinamis menggunakan PHP dan MySQL*. C.V ANDI OFFSET. Yogyakarta.
- Behrouz A. Forouzan ,TCP/IP Protokol Suite Penerbit Graw Hill
- Bunafit, Nugroho, 2006. *Membuat Aplikasi Sistem Pakar dengan PHP dan My SQL dengan PHP dan MySQL dengan Editor Dreamweaver*. Ardana Media, Yogyakarta.
- CCNA, *Todd Lammle*  
pengarang elekmedia komputindo, 2007
- Coleman Curtis. *Case Study: An Evolution of Putting Security into SDLC*.  
Available:  
[http://www.owasp.org/docroot/owasp/misc/COLEMAN-Putting\\_Security\\_IntoSDLS-OWASP\\_v2.ppt](http://www.owasp.org/docroot/owasp/misc/COLEMAN-Putting_Security_IntoSDLS-OWASP_v2.ppt)
- Gullett, David, Snort 2.9.0.5 and Snort Report 1.3.1 on Ubuntu 10.04 LTS  
Installation Guide. United States: Symmetrix Technologies. 2011
- Karen Scarfone Peter Mell, 2007, dalam Buku *Recommendations of the National Institute of Standards and Technology (NIST) dalam Guide to Intrusion Detection and Prevention Systems*
- Nafisah Syifaun, 2003. *Perancangan Aplikasi*. Grafika Komputer. Yogyakarta: Graha Ilmu
- Onno W. Purbo, 2007. *Buku Pintar Internet TCP/IP*. PT. Elex Media Komputindo. Jakarta.
- Raghavendra K & Sumith Nireshwalya, 2012 Dalam jurnal Application Layer Security Issues and Its Solutions,
- Von Hagen, William. *Ubuntu Linux Bible*. Indiana: Wiley Publishing, Inc. 2007
- Waskita, Adi. Hiswendari, Lely. *Local Area Network: Basic*. Jakarta. 2004
- Wahsheh, Luay A dan Foss, Jim Alves 2008, *Security Policy Development: Towards a life- cycle and Logic-Based Verification Model*. USA
- William Stallings. 2011 *Network Security Essentials: Applications and Standarts Fourt Edition*. Prentice Hall.