BAB III

ANALISA JARINGAN BERJALAN

3.1. Tinjauan Perusahaan

PT.Indo Pratama Teleglobal merupakan salah satu vendor infrastruktur VSAT. Dimana VSAT merupakan salah satu perangkat koneksi jaringan skala luas maka PT. Indo Pratama Teleglobal menjadi salah satu Vendor yang melayani barang dan jasa dalam pemasangan atau Instalasi VSAT.

3.1.1. Sejarah Perusahaan

PT. Indo Pratama Teleglobal (Teleglobal) Didirikan pada tahun 2000 dan tak lama kemudian akan menjadi salah satu pemimpin di grosir internet berbasis satelit untuk terminasi internasional dan originasi. Hal itu dibentuk sebagai tanggapan dari, jaringan internet komputer berkembang, dan telekomunikasi, yang berbasis di Asia , dengan Nomor SIUP (surat Ijin Usaha Perdagangan) : 01351-01/PB/P/1.824.271

Teleglobal mempertahankan pelanggan utama dan teknis pusat layanan di Jakarta, dengan kantor dan HUB jaringan di Jakarta. Teleglobal memberikan layanan berupa:

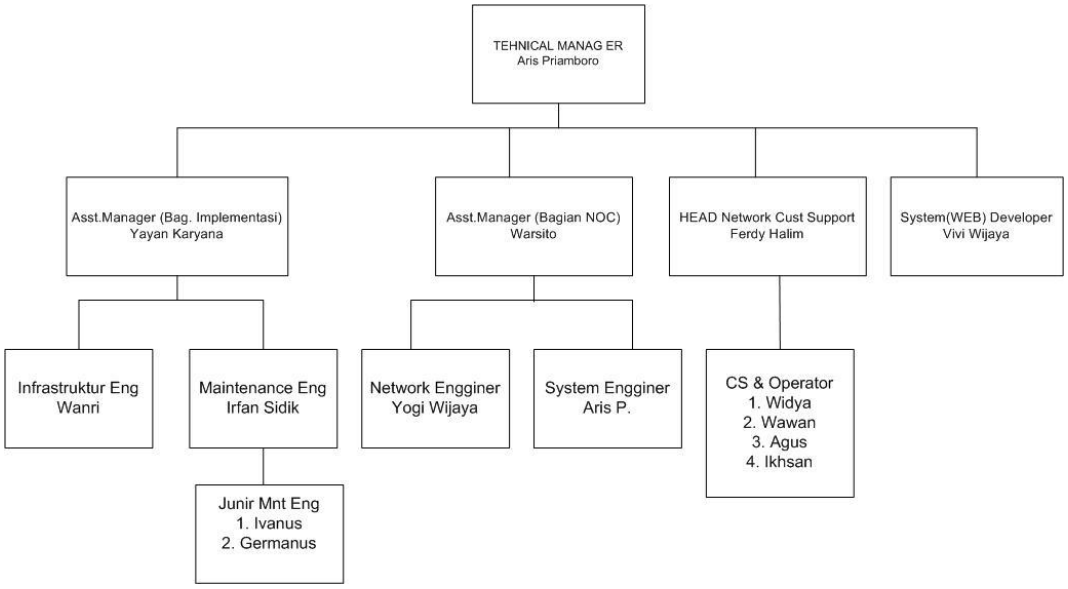
1. Layanan *Internet* berbasis: ISP.
2. Infrastruktur penyedia: FO, VSAT, *Wireless*
3. Sistem Integrasi: Data *Center*.

Visi PT. Indo Pratama Teleglobal : Menuju dunia penyedia pelayanan telekomunikasi Internasional.

Misi PT.Indo Pratama Teleglobal : Membangun jaringan *Internet* dan *provider* skala lokal maupun interlokal.

Jenis jaringan yang telah di bangun meliputi: jaringan *internet* berbasis FO, VSAT yang mecakup sampai ke negara tetanga.

3.1.2. Struktur Organisasi dari NOC PT.Indo Pratama Teleglobal



Sumber : PT. Indo Pratama Teleglobal Per Januari 2015

Gambar III.1 Struktur Organisasi NOC PT. Indo pratama Teleglobal

3.2 Manajemen Jaringan

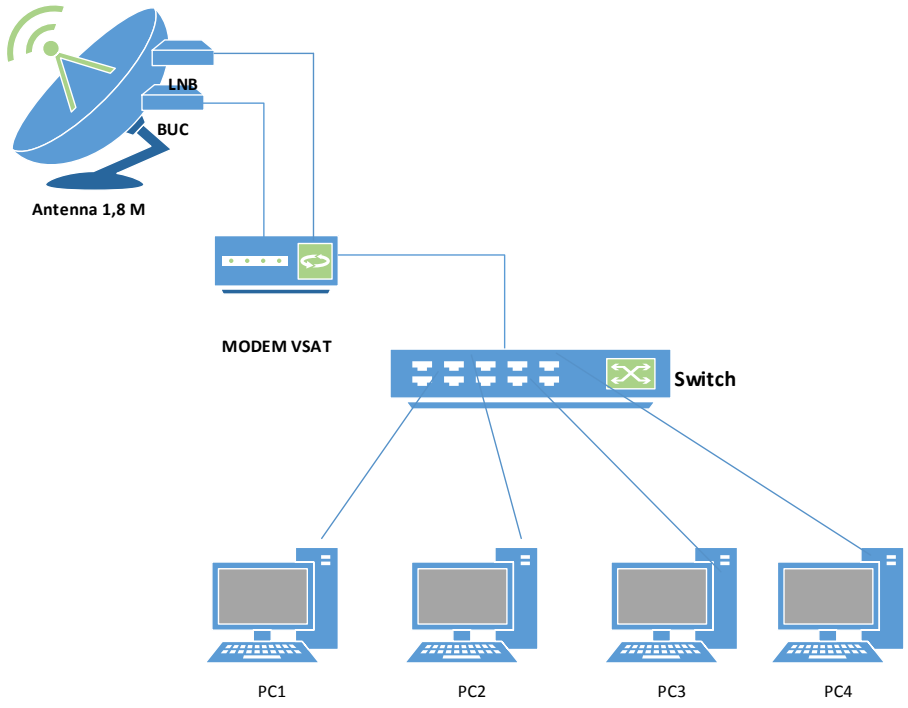
3.2.1. Topologi Jaringan

Topologi yang di gunakan pada PT. Indo Pratama Teleglobal untuk seluruh client/pelanggan yaitu topologi *Star/*bintang. Karena semua *client* / pelanggan terkoneksi melalui HUB *Vsat*. Setiap client mendapatkan 5 buah Public IP yang dapat digunakan di PC / *Server*, tetapi umumnya pelanggan yang hanya membutuhkan koneksi internet cukup diberikan *Private* IP kelas C, sementara proses NAT berada di sisi Modem.

3.2.2. Asiterktur Jaringan

1. Arsitektur Jaringan *Client* atau pelanggan

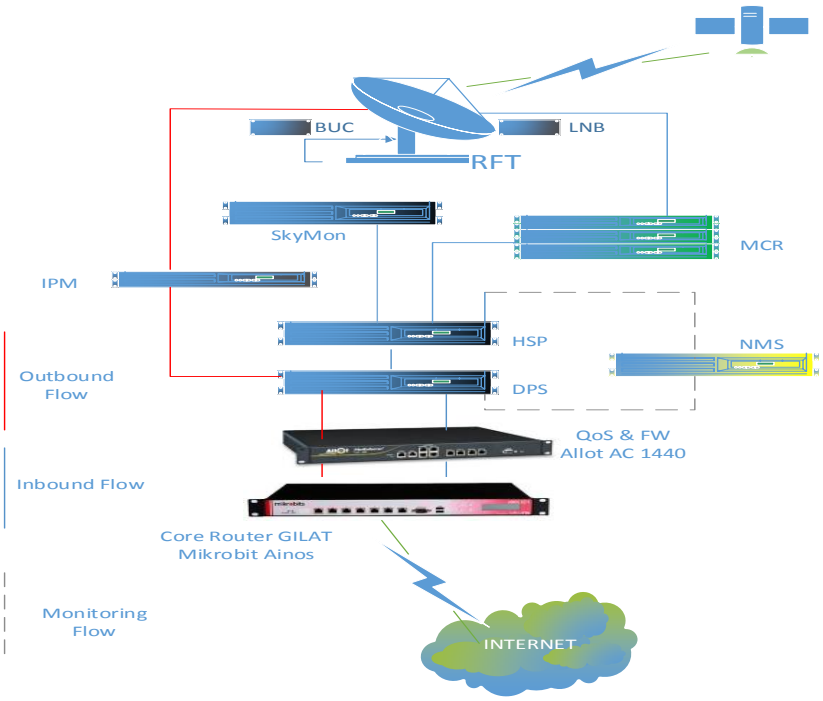
   Hasil analisa, *client* rata-rata menggunakan 4 s/d 10 buah PC , dan sebuah *Switch* ataupun *Router*, berikut contoh gambar arsitektur jaringan *client* yang sudah terintegrasi dengan VSAT.



Gambar III.2 Contoh Arsitektur jaringan *Client* / pelanggan

2. Arsitektur jaringan HUB VSAT

Pada sistem jaringan HUB PT. Indo Pratama Teleglobal menggunakan VSAT HUB yang menghubungkan internet dengan *client*/pelanggan di remote site. Terdapat *Core Router* GILAT yang berfungsi mengatur alur routing dari dan untuk *client*/pelanggan. Setelah Router terdapat sebuah perangkat Allot yang berfungsi sebaga Bandwidth management dan *Firewall*, setelah itu data masuk ke DPS (*Data Protocol Server*), disini data yang lewat dirubah ke MPEG 2 frames atau disebut *Backbone Packets*, setelah di rubah ke *Backbone Packet*, selanjutnya dikonversikan menjadi LBand oleh IPM untuk kemudian di teruskan ke pelanggan melalui *satelit*.

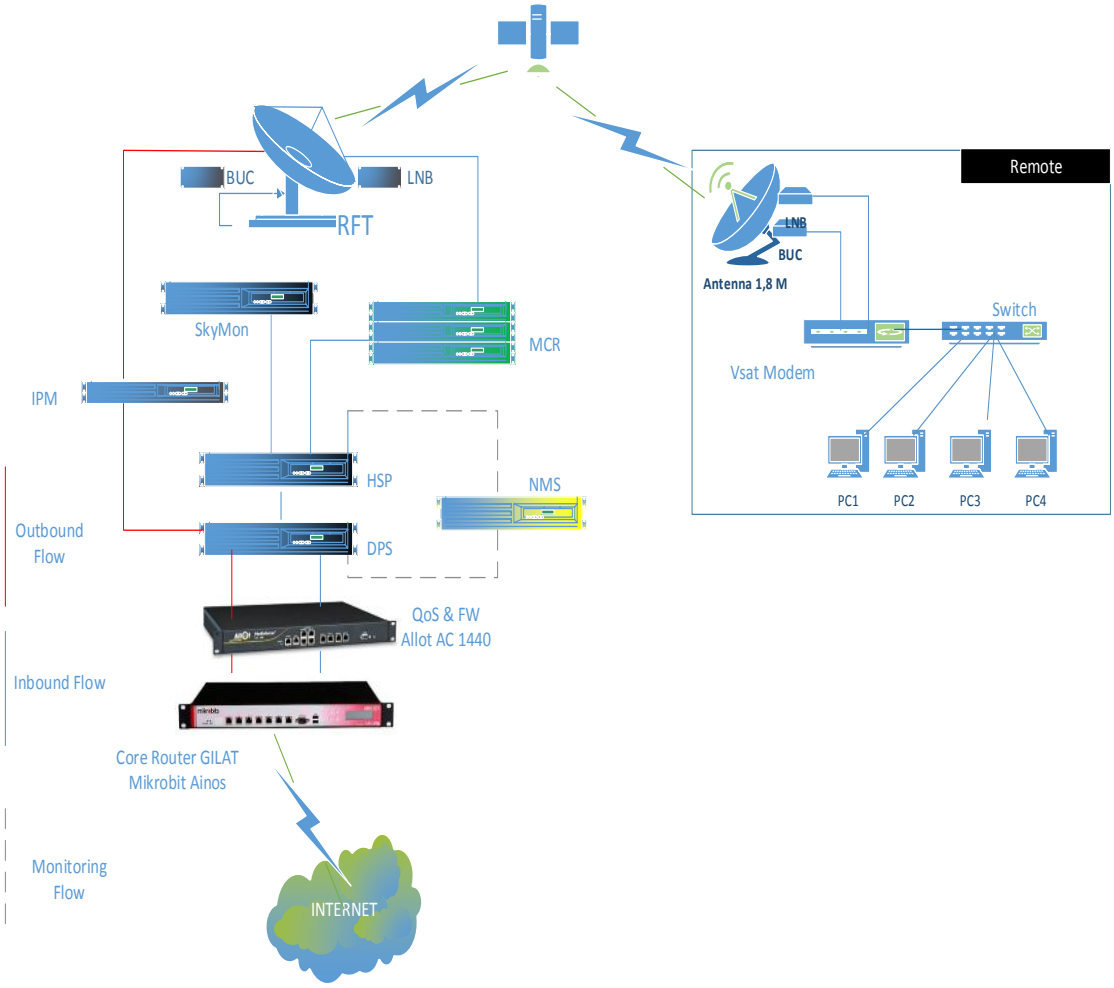


Gambar III.3 Arsitektur Jaringan HUB VSAT GILAT PT.Indo Pratama Teleglobal

3.2.3 Skema Jaringan

Skema Jaringan VSAT Pada PT.Indo Pratama Teleglobal yang terhubung dengan *Client*/pelanggan.

Berikut adalah contoh gambar skema jaringan *Client*/ pelanggan yang sudah terinstallasi VSAT dan terkoneksi dengan HUB.



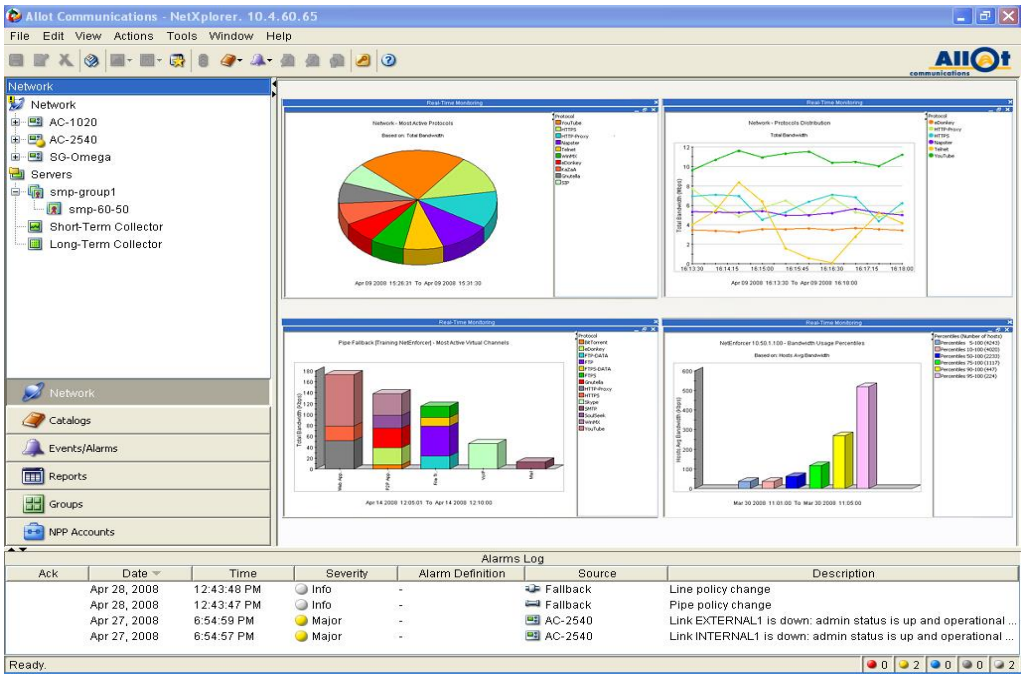
Gambar III.4 Skema Jaringan VSAT pada HUB ke *Client*/Pengguna

3.2.4. Keamanan Jaringan

Berikut sistem keamanan yang diterapkan pada jaringan yang berjalan di sisi HUB yaitu PT.Indo Pratama Teleglobal, di HUB menggunakan sebuah perangkat yaitu *Allot Net Enforcer*. Dimana fitur *Allot Net Enforcer* antara lain :

1. Sebagai *bandwidth* management (*Inbound QOS*).
2. Pemantauan lalu lintas *real-time* dan alarm otomatis memungkinkan pemecahan masalah yang cepat dan akurat dengan kemampuan untuk proses *Troubleshooting*.
3. Sistem perlindungan *all-in*, dari *level* IP sampai dengan applikasi.

Contoh report realtime yang diberikan oleh Allot Net Enforcer :



Gambar III.5 Report view allot netenforcer

Sumber : *Allot Netenforcer* PT. Indo Pratama Teleglobal April 2008

3.2.5. Spesifikasi Hardware dan Software Jaringan

1. *Hardware*

Adapun beberapa *hardware* yang di gunakan antara lain:

a. *Server*

Tabel III.1 Spesifikasi komputer server

No	HUB	Spesifikasi	Ip Address
1	Server NMS	Xeon QuadCore, Ram 8GB, HD 360 GB(Raid 5 Mode), OS: Windows 2003 Server SP2	172.16.x.x
2.	MRTG-Server	Xeon QuadCore, Ram 4GB, HD 360 GB(Raid 5 Mode) OS: Centos 5.1	202.55.x.x
3.	GILAT Hub Server	DPS,HSP,MCR,IPM Xeon QuadCore, Ram 8GB, HD 360 GB(Raid 5 Mode),	172.16.x.x
4	Bandwidth Management	Allot Netenforce AC-1440, Througput 2 Gbps	172.17.x.x

b. Antena

Tabel III.2 Spesifikasi Antena

Antena	Spesifikasi
Client	1,8 meter
Hub	9 meter

c. *Switch* (*Remote Site*)

d. *Modem Gilat (Remote Site)*

Type SkyEdge IP.

Spesifikasi :

1) CPU : Power QUICC 133 Mhz,
2) Memory : Flash 16 MB, DDR2 64MB
3) Services : Support 2 Vlans, and 512 TCP Connection

4) Power Supply : (AC) 90-240V
5) IB Channel Rate : 128 s/d1536 Ksps (Kilo symbol per second)
6) Data Rate : UPLink, upto 1,2 Mbps, DownLink upto 7.5 Mbps

e. Perangkat Lunak (*Software)*

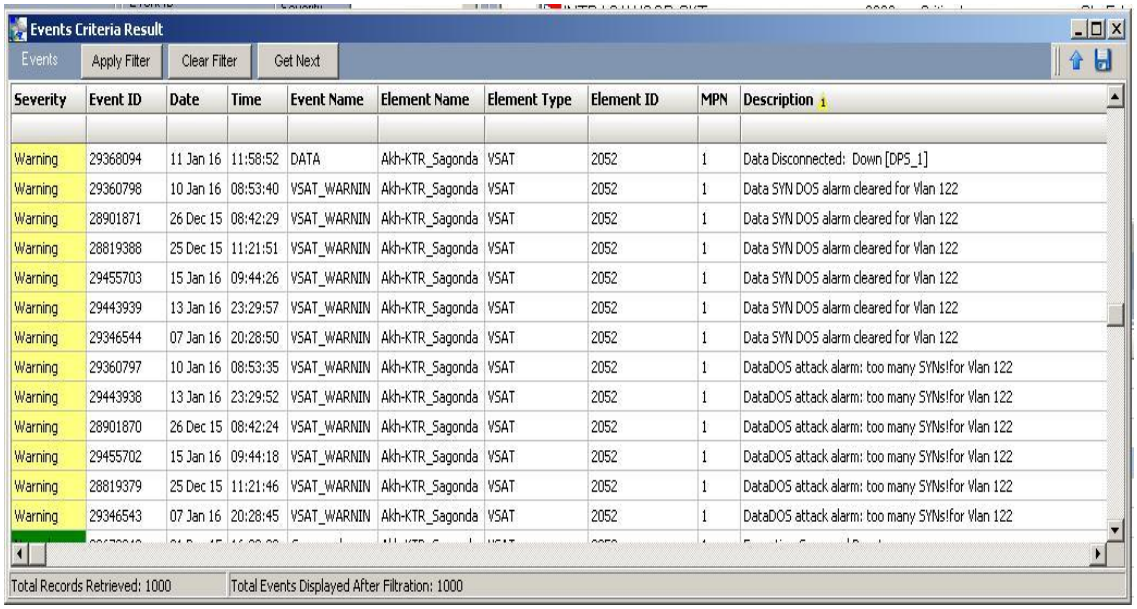
Perangkat lunak (*software)* yang digunakan pada HUB GILAT, terdiri dari sistrem operasi, dan juga perangkat lunak pendukung lainnya yang digunakan seperti:

a. Linux Distro Centos 7
b. SO *server*
   1.) Windows server 2003
c. SO NMS-*Client*
   1.) Windows XP

3.2. Permasalahan Sistem Jaringan

Dari hasil analisa yang penulis lakukan, terdapat beberapa kendala dalam pemberian data yaitu:

a. Banyaknya *alert* atau event di NMS *server* karena *DoS-attack* yang menyebabkan untuk *access browsing* jadi lambat dan tidak setabil.



Severity	Event ID	Date	Time	Event Name	Element Name	Element Type	Element ID	MPN	Description
Warning	29368094	11 Jan 16	11:58:52	DATA	Akh-KTR_Sagonda	VSAT	2052	1	Data Disconnected: Down [DP5_1]
Warning	29360798	10 Jan 16	08:53:40	VSAT_WARNIN	Akh-KTR_Sagonda	VSAT	2052	1	Data SYN DOS alarm cleared for Vlan 122
Warning	28901871	26 Dec 15	08:42:29	VSAT_WARNIN	Akh-KTR_Sagonda	VSAT	2052	1	Data SYN DOS alarm cleared for Vlan 122
Warning	28819388	25 Dec 15	11:21:51	VSAT_WARNIN	Akh-KTR_Sagonda	VSAT	2052	1	Data SYN DOS alarm cleared for Vlan 122
Warning	29455703	15 Jan 16	09:44:26	VSAT_WARNIN	Akh-KTR_Sagonda	VSAT	2052	1	Data SYN DOS alarm cleared for Vlan 122
Warning	29443939	13 Jan 16	23:29:57	VSAT_WARNIN	Akh-KTR_Sagonda	VSAT	2052	1	Data SYN DOS alarm cleared for Vlan 122
Warning	29346544	07 Jan 16	20:28:50	VSAT_WARNIN	Akh-KTR_Sagonda	VSAT	2052	1	Data SYN DOS alarm cleared for Vlan 122
Warning	29360797	10 Jan 16	08:53:35	VSAT_WARNIN	Akh-KTR_Sagonda	VSAT	2052	1	DataDOS attack alarm: too many SYNs!for Vlan 122
Warning	29443938	13 Jan 16	23:29:52	VSAT_WARNIN	Akh-KTR_Sagonda	VSAT	2052	1	DataDOS attack alarm: too many SYNs!for Vlan 122
Warning	28901870	26 Dec 15	08:42:24	VSAT_WARNIN	Akh-KTR_Sagonda	VSAT	2052	1	DataDOS attack alarm: too many SYNs!for Vlan 122
Warning	29455702	15 Jan 16	09:44:18	VSAT_WARNIN	Akh-KTR_Sagonda	VSAT	2052	1	DataDOS attack alarm: too many SYNs!for Vlan 122
Warning	28819379	25 Dec 15	11:21:46	VSAT_WARNIN	Akh-KTR_Sagonda	VSAT	2052	1	DataDOS attack alarm: too many SYNs!for Vlan 122
Warning	29346543	07 Jan 16	20:28:45	VSAT_WARNIN	Akh-KTR_Sagonda	VSAT	2052	1	DataDOS attack alarm: too many SYNs!for Vlan 122

Gambar III.6 Virus yang broadcast dari sisi Cutomer

b. Dengan banyak *website-website* yang menggandung unsur pornografi dan *website-website* yang di anggap berbahaya baik untuk user sendiri atau dalam segi keamanan jaringan vsat.

3.3. Alternatif Pemecahan Masalah

Dari permasalahan yang terdapat di atas, maka berikut adalah alternatif pemecahan masalahnya:

a. Dengan diimplementasikan *Unbound* makan untuk terjadinya *DoS-Attack* di sisi customer akan menjadi lebih kecil karena akan di *block* langsung oleh *Unbound* untuk access ke *website* yang dianggap berbahaya.

b. Implementasikan DNS *Unbound* sebagain memvalidasi *rekursif* dan *caching* DNS *server* yang dirancang untuk kinerja tinggi dan DNS Filtering dimana fungsinya adalah untuk mem*block website-website* yang dianggap mengandung unsur-unsur dan content pornografi dan *web* yang menyebarkan *virus malware* dan *spyware*.