IPS (Intrusion Prevention System) Untuk Mencegah Tindak Penyusupan / Intrusi

Jutono Gondohanindijo
Fakultas Ilmu Komputer Universitas AKI

Abstract

In a complex computer network, data security and authentication process is a must. To ensure that the data is accessible, and the process by which the right to access the data, then the rules or protocols that have a good mechanism but it is very compact and easy to use needs to be applied on the network.

IPS (Intrusion Prevention System) is a network security tools that monitor system or network activity from undesirable behavior (anomaly) and can react in real-time to stop these activities. IPS born is the development of IDS (Intrusion Detection System).

In this study will be presented how to use IPS in preventing intrusion into our computer connected to the global network called the Internet in order to stay safe.

Key words **:** *IPS, System, Crime, Intrusion, Detection, Integrity, Security, Network*

1. Pendahuluan

Sistem Keamanan Komputer telah menjadi fokus utama dalam dunia Jaringan Komputer, hal ini disebabkan tingginya ancaman yang mencurigakan (*suspicious threat*) dan serangan dari Internet. Keamanan Komputer (*Security*) merupakan salah satu kunci yang dapat mempengaruhi tingkat Reliability (termasuk performance dan availability) suatu internetwork (Deris S., A. Hanan, M. Yazid, 2010).

Intrusion adalah aktivitas tidak sah atau tidak diinginkan yang mengganggu konfidensialitas, integritas dan atau ketersediaan dari informasi yang terdapat di sebuah sistem. IDS akan memonitor lalulintas data pada sebuah jaringan atau mengambil data dari berkas log. IDS akan menganalisa dan dengan algoritma tertentu akan memutuskan untuk memberi peringatan kepada seorang administrator jaringan atau tidak.

1.1. IPS (Intrusion Prevention System)

Intrusion Prevention System (IPS), adalah pendekatan yang sering digunakan untuk membangun system keamanan komputer, IPS mengkombinasikan 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, disaat attack telah teridentifikasi, IPS akan menolak akses (block) dan mencatat (log) semua paket data yang teridentifikasi tersebut. Jadi IPS bertindak sepeti layaknya Firewall yang akan melakukan *allow* dan *block* yang dikombinasikan seperti IDS yang dapat mendeteksi paket secara detail. IPS menggunakan *signatures* untuk mendeteksi di aktivitas *traffic* di jaringan dan terminal, dimana pendeteksian paket yang masuk dan keluar (*inbound-outbound*) dapat di cegah sedini mungkin sebelum merusak atau mendapatkan akses ke dalam jaringan lokal. Jadi *early detection* dan *prevention* menjadi penekanan pada IPS ini (E. Carter, 2006).

Namun implementasi IPS pada jaringan *internetwork* sangat dipengaruhi oleh beberapa faktor lainnya. Faktor teknis menjadi kendala utama dalam implementasi ini, karena IPS adalah salah satu bagian dalam system keamanan yang dibangun, hendaknya memperhatikan isu-isu yang ada dalam jaringan komputer. Dalam tulisan ini, penulis mencoba menjabarkan secara umum apa saja faktor-faktor utama yang menjadi perhatian utama dalam implementasi teknologi ini, serta solusi yang dapat dilakukan sebagai pemecahannya.

Jika kita lihat dan beranjak dari data CSI/FBI survey (Robert Richardson, 2008), saat ini telah banyak perusahaan yang membelanjakan uangnya untuk terhindar dari masalah keamanan ini dan sementara itu juga untuk mengamankan sistemnya, banyak perusahaan tersebut telah menggunakan system dengan mengkombinasikan beberapa teknologi system keamanan, dimana hampir 69%nya menggunakan solusi dari *Intrusion Prevention System* (IPS).

1.2. IDS (*Intrusion Detection System*)

IDS (*Intrusion Detection System*) adalah sebuah aplikasi perangkat lunak atau perangkat keras yang dapat mendeteksi aktivitas yang mencurigakan dalam sebuah

sistem atau jaringan. IDS digunakan untuk mendeteksi aktivitas yang mencurigakan dalam sebuah sistem atau jaringan (Wardhani, 2011).

IDS (*Intrusion Detection System*) sendiri mempunyai beberapa pengertian yaitu:

a. Sistem untuk mendeteksi adanya *intrusion* yang dilakukan oleh *intruder* (pengganggu atau penyusup) dalam jaringan.

   Pada awal serangan, intruder biasanya hanya mengexplore data. Namun, pada tingkat yang lebih serius intruder berusaha untuk mendapat akses ke sistem seperti membaca data rahasia, memodifikasi data tanpa permisi, mengurangi hak akses ke sistem sampai menghentikan sistem.

b. Sistem keamanan yang bekerja bersama Firewall untuk mengatasi Intrusion.

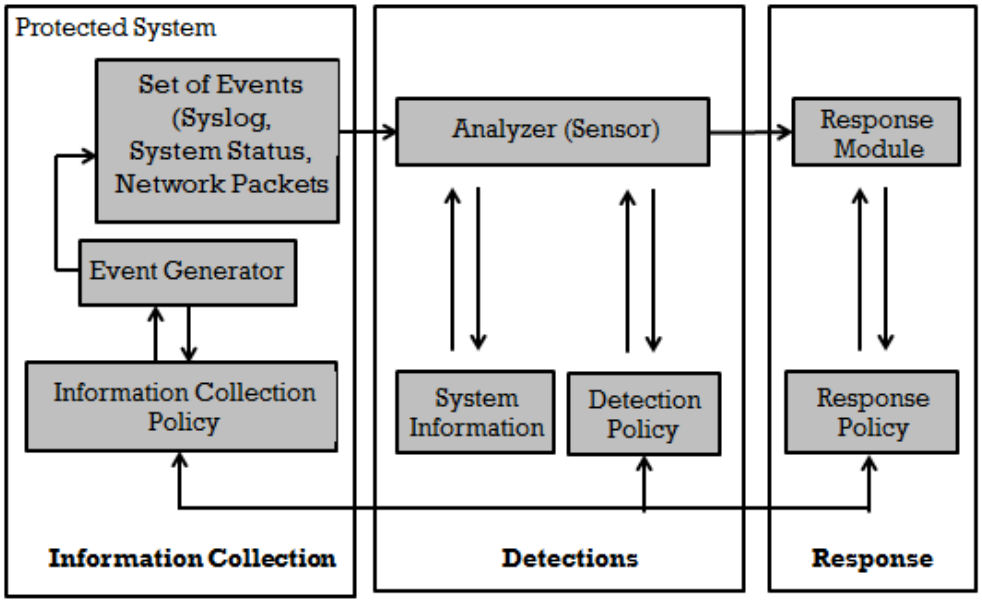
   Intrusion itu sendiri didefinisikan sebagai kegiatan yang bersifat *anomaly, incorrect, inappropriate* yang terjadi di jaringan atau di host tersebut. Intrusion tersebut kemudian akan diubah menjadi *rules* ke dalam IDS (*Intrusion Detection System*).

c. Sebuah aplikasi perangkat lunak atau perangkat keras yang dapat mendeteksi aktivitas yang mencurigakan dalam sebuah sistem atau jaringan.

1.3. Cara kerja IDS

IDS melindungi sistem komputer dengan mendeteksi serangan dan menghentikannya. Awalnya, IDS melakukan pencegahan intrusi. Untuk itu, IDS mengidentifikasi penyebab intrusi dengan cara membandingkan antara event yang dicurigai sebagai intrusi dengan signature yang ada. Saat sebuah intrusi telah terdeteksi, maka IDS akan mengirim sejenis peringatan ke administrator. Langkah selanjutnya dimulai dengan melakukan policy terhadap administrator dan IDS itu sendiri.

Komponen yang menyusun kerja sebuah IDS bisa dilihat pada diagram berikut (Sundaram, 1996) :



Gambar 1 : Komponen Kerja Sebuah IDS

Ada beberapa cara bagaimana IDS bekerja. Cara yang paling populer adalah dengan menggunakan pendeteksian berbasis signature (seperti halnya yang dilakukan oleh beberapa antivirus), yang melibatkan pencocokan lalu lintas jaringan dengan basis data yang berisi cara-cara serangan dan penyusupan yang sering dilakukan oleh penyerang. Sama seperti halnya antivirus, jenis ini membutuhkan pembaruan terhadap basis data signature IDS yang bersangkutan.

Cara lainnya adalah dengan mendeteksi adanya anomali, teknik yang lainnya adalah dengan memantau berkas-berkas sistem operasi, yakni dengan cara melihat apakah ada percobaan untuk mengubah beberapa berkas sistem operasi, utamanya berkas log. Teknik ini seringnya diimplementasikan di dalam HIDS (*Host-Based IDS*), selain tentunya melakukan pemindaian terhadap log sistem untuk memantau apakah terjadi kejadian yang tidak biasa.

Beranjak dari masalah kemanan komputer, penelitian ini memberikan gambaran penggunaan IPS yang semakin hari semakin banyak dikembangkan dan banyak diimplementasikan dalam antivirus seperti Symantec. IPS adalah pengembangan

lanjut dari IDS (Intrusion Detection System).

1.4. Tujuan dan Manfaat Penelitian

Tujuan umum penelitian ini adalah untuk memahami cara kerja IPS dan bagaimana mengimplementasikannya, sedangkan manfaatnya adalah mengetahui implementasi IPS dalam mengamankan sistem komputer, serta mengetahui apa saja bentuk IPS dan cara memanfaatkannya.

2. Metodologi

Dalam penulisan penelitian ini penulis mendapatkan data dari berbagai sumber yang relevan sebagai bahan untuk penyusunan penelitian ini dengan jenis data:

a. Data Primer

   Data Primer diperoleh langsung melalui proses pengamatan dan wawancara secara langsung dengan sumber atau pihak yang bersangkutan (responden) yang siap untuk diolah (Wirartha, 2006, Hal.35). Dalam penelitian ini data primer diperoleh melalui wawancara dan observasi pada Instansi Pemerintah maupun Swasta yang bergerak dibidang bisnis maupun non bisnis pada bagian pengolahan datanya, data berupa dokumen informasi serta wawancara praktisi / pakar teknologi dibidang informasi yang berhubungan dengan aplikasi IPS.

b. Data Sekunder

   Data sekunder adalah data yang diperoleh dan dikumpulkan secara tidak langsung yaitu melalui buku-buku, majalah – majalah, dan semua media yang berkaitan dengan permasalahan pada objek penelitian (Wirartha, 2006, Hal.35).

2.1. Metode Pengumpulan Data :

Sesuai dengan jenis data dan maksud serta tujuan penyusunan penulisan ini maka dalam menyusun penelitian, penulis menggunakan metode sebagai berikut:

a. Metode Wawancara / *Interview*

   Merupakan salah satu metode pengumpulan data dengan jalan komunikasi yaitu dengan kontak dan hubungan pribadi antara pengumpul data dengan sumber data (Wirartha, 2006, Hal.37). Penulis melakukan wawancara pada personal yang ada di bagian Pengolahan Data serta pakar

teknologi informasi yang ada di instansi / lembaga terkait.

b. Metode Pengamatan

Data dapat diperoleh melalui pengamatan terhadap gejala yang diteliti. Dalam hal ini, panca indra manusia (penglihatan dan pendengaran). hasil pengamatan tersebut ditangkap kemudian di analisis untuk menjawab masalah penelitian (Wirartha, 2006, Hal.37). Dari pengamatan ini, penulis mendapatkan data dari dokumen-dokumen informasi yang ada, tampilan media elektronik (komputer) serta dari tanya jawab langsung dengan nara sumber.

c. Studi Pustaka

Metode ini dilakukan dengan cara mempelajari literatur – literatur yang ada hubungannya dengan objek penelitian (Wirartha, 2006, Hal.36). Dalam hal ini referensi yang digunakan adalah buku – buku dan e-book berkaitan dengan tema penelitian.

3. Pembahasan

3.1. Kinerja IPS

Intrusion prevention system (IPS) bertugas untuk memonitor paket-paket data (data packets) jaringan dari adanya aktivitas mencurigakan dan mencoba melakukan aksi-aksi tertentu menggunakan kebijakan-kebijakan (policy) tertentu (Xinyau Zhang, 2007). IPS akan mengirimkan sebuah peringatan (alert) kepada network atau system administrator ketika suatu hal yang mencurigakan terdeteksi, memungkinkan administrator dapat memilih sebuah tindakan untuk diambil ketika terjadi sebuah event. Intrusion prevention system dapat memonitor seluruh jaringan, wireless network protocol, perilaku jaringan (network behaviour) dan traffic sebuah komputer. Setiap IPS menggunakan metode deteksi tertentu untuk menganalisis resiko.

Tergantung dari model IPS yang digunakan beserta fitur-fiturnya, sebuah intrusion prevention system dapat mendeteksi berbagai macam pelanggaran keamanan. Beberapa diantaranya dapat mendeteksi penyebaran malware pada sebuah jaringan, duplikasi file-file besar di antara dua komputer, dan mendeteksi adanya aktivitas mencurigakan seperti aktivitas port scanning.

Setelah IPS membandingkan masalah yang muncul dengan aturan keamanan (security rule) yang telah dibuat, maka IPS akan mencatat setiap event dan akan mencatat frekuensi kemunculan event. Jika seorang network administrator mengkonfigurasikan IPS untuk menjalankan tindakan tertentu berdasarkan kejadian, intrusion prevention system kemudian akan menjalankan perintah yang telah diberikan tersebut. Sebuah basic alert akan dikirimkan pada administrator, sehingga administrator dapat merespon secara tepat atau melihat informasi tambahan pada IPS jika diperlukan.

Ada beberapa metode IPS (Intrusion Prevention System) melakukan kebijakan apakah paket data yang lewat layak masuk atau keluar dalam jaringan tersebut :

1. Signature-based Intrusion Detection System

   Pada metode ini, telah tersedia daftar signature yang dapat digunakan untuk menilai apakah paket yang dikirimkan berbahaya atau tidak. Sebuah paket data akan dibandingkan dengan daftar yang sudah ada. Metode ini akan melindungi sistem dari jenis-jenis serangan yang sudah diketahui sebelumnya. Oleh karena itu, untuk tetap menjaga keamanan sistem jaringan komputer, data signature yang ada harus tetap ter-update.

2. Anomaly-based Intrusion Detection System

   Pada metode ini, terlebih dahulu harus melakukan konfigurasi terhadap IDS dan IPS, sehingga IDS dan IPS dapat mengetahui pola paket seperti apa saja yang akan ada pada sebuah sistem jaringan komputer. Sebuah paket anomali adalah paket yang tidak sesuai dengan kebiasaan jaringan komputer tersebut. Apabila IDS (Intrusion Detection System) dan IPS (Intrusion Prevention System) menemukan ada anomali pada paket yang diterima atau dikirimkan, maka IDS dan IPS akan memberikan peringatan pada pengelola jaringan (IDS) atau akan menolak paket tersebut untuk diteruskan (IPS). Untuk metode ini, pengelola jaringan harus terus-menerus memberi tahu IDS dan IPS bagaimana lalu lintas data yang normal pada sistem jaringan komputer tersebut, untuk menghindari adanya salah penilaian

oleh IDS (Intrusion Detection System) atau IPS (Intrusion Prevention System).

Intrusion prevention system mengkombinasikan kemampuan network based IDS dengan kemampuan firewall, sehingga selain mendeteksi adanya penyusup juga bisa menindaklanjuti dengan melakukan pengeblokan terhadap IP yang melakukan serangan. Beberapa IPS opensource yang dikenal :

1. Portsentry
   Portsentry digunakan untuk melakukan pengeblokan IP address yang melakukan scanning port dengan menggunakan fasilitas dari firewall atau teknik null route.
2. Sshdfilter
   Sshdfilter digunakan untuk melakukan blocking IP address yang melakukan ssh brute forcing.
3. Snort
   Snort di gandeng dengan *blockit* dan firewall merupakan NIPS yang mampu melakukan blocking IP address terhadap beragam serangan yang di definisi di signature snort.

Hal yang perlu diperhatikan dalam pemasangan IPS, saran yang diberikan jangan memasang IPS di gateway karena sangat beresiko membuat nilai usability service yang ditawarkan menjadi sangat rendah. Terapkan IPS di host – host di jaringan yang sifatnya krusial dengan signature detection yang benar-benar akurat untuk mendeteksi bugs sekuritas yang sifatnya critical (Deris S., A. Hanan, M. Yazid, 2010).

3.2. Tipe-tipe IPS

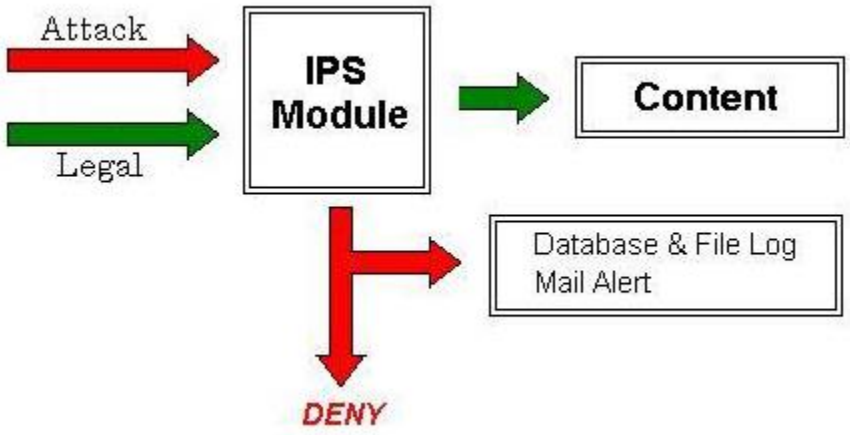
1. Host Based IPS yang berada pada spesifik IP address, biasanya terdapat pada single komputer.
2. Network IPS yang berguna untuk mencegah penyusupan pada spesifik network.
3. Content Spesific IPS yang memeriksa kontent dari suatu paket dan mencegah berbagai macam serangan seperti serangan worm.
4. Protocol Analysis Menganalisa berbagai macam application layer network protocol seperti http dan ftp.
5. Rated Based Berguna mencegah denial of service. Berguna untuk

memonitoring dan dan mempelajari keadaan normal network. RBIPS dapat memonitoring taffic TCP, UDP, ARP Packets, koneksi per detik, paket per koneksi

IPS memiliki NIPS (Network Based Intrusion Prevention System). IPS tidak hanya mendeteksi adanya serangan tetapi dia akan otomatis melakukan aksi, biasanya dengan block traffic yang ada. NIPS merupakan gabungan dari NIDS (Network Based Intrusion Detection System) dan Firewall.

NIPS (Network Based Intrusion Prevention System) adalah sebuah pengamanan jaringan yang dapat mendeteksi dan melakukan blocking pada serangan atau intrusion yang mengganggu jaringan. NIPS biasanya dikembangkan selayaknya switch dan router. NIPS melakukan deteksi ke seluruh paket data yang akan masuk ke dalam jaringan, dengan cara melakukan pengecekkan pola serangan ataupun pattern dari paket data tersebut. Ketika NIPS mendeteksi sebuah serangan, NIPS (Network Based Intrusion Prevention System) akan langsung melakukan tindakan yang dapat berupa blocking paket – paket data tersebut.

3.3. NIPS (Network Based Intrusion Prevention System)



Gambar 2. Network Based Intrusion Prevention System (NIPS)

Pada masa sekarang ini IDS (Intrusion Detection System) dan IPS (Intrusion Prevention System) telah berkembang. Kedua metode keamanan tersebut dijadikan satu kesatuan sehingga kinerja pengamanannya menjadi lebih maksimal. Sebuah vendor telah mengembangkan teknologi tersebut dan mengimplementasikannya ke dalam sebuat alat yang disebut IDPS (Intrusion Detection and Prevention System). IDPS (Intrusion Detection and Prevention System) menjadi sistem pendeteksi dan pencegahan dari gangguan – gangguan. Dengan adanya IDPS (Intrusion Detection and Prevention System), kinerja IDS (Intrusion Detection System) dan IPS (Intrusion Prevention System) menjadi lebih baik ketika teknologi keamanan tersebut diintegrasikan dalam sebuah alat. IDPS (Intrusion Detection and Prevention System) dapat berfungsi sebagai sebuah virtual device.

IDPS (Intrusion Detection and Prevention System) sangat perlu diketahui akan pentingnya diterapkan pada masa sekarang ini, hal tersebut dikarenakan IDPS (Intrusion Detection and Prevention System) memiliki beberapa kemampuan, yaitu :

3. Mencegah serangan atau gangguan dalam jaringan

IDPS adalah peralatan keamanan yang kompleks yang menggunakan berbagai jenis teknologi pendeteksi untuk menemukan gangguan yang berupa program-program jahat yang masuk kedalam jaringan dan menghentikannya sebelum worm, trojan, virus atau program jahat lainnya dapat merusak sistem.

Dengan hanya memasang IDS, sistem pendeteksi gangguan saja, alat tersebut hanya akan memberikan *alarm* peringatan adanya keanehan atau gangguan pada sistem, dan administrator jaringan yang harus menyelidiki code mencurigakan yang dimaksud dan memutuskan tindakan selanjutnya. Bila selain IDS dipasangi juga IPS, maka *code* jahat yang ditemukan tersebut akan langsung dihentikan secara otomatis.

IDPS melakukan kedua hal tersebut dengan menghentikan koneksi jaringan/*user* yang menyerang sistem, memblok *user account* yang berbahaya, IP *address* atau atribut lain dari pengaksesan ilegal terhadap server atau aset lain dalam jaringan. Atau dapat pula dengan mematikan seluruh akses ke *host*, *service*, aplikasi atau aset-aset lain dalam jaringan.

Beberapa IDPS cukup baik dalam meningkatkan kemampuan pengamanannya melawan serangan berbahaya.

1. Menghentikan serangan melalui *re-configuring* peralatan kontrol keamanan pada *network*, seperti *router* dan *firewall*, untuk memblok akses yang bersifat ilegal.
2. Menghentikan serangan melalui pemasangan *patch* pada *host* untuk menutup *vulnerabilities*.
3. Menghentikan serangan melalui penghapusan *code* jahat yang ditemukan seperti men-*deletefile attachment* dalam e-mail.

4. Memberitahu administrator jaringan tentang adanya gangguan keamanan

IDPS akan memberitahukan administrator jaringan tentang segala sesuatu yang menyangkut pelanggaran peraturan keamanan atau serangan yang terdeteksi.

Pemberitahuan tersebut dapat melalui e-mail, *web page*, pesan dalam monitor IDPS *user*, perangkap SNMP (*Simple Network Management Protokol*), pesan *syslog*, atau program yang dibuat oleh *user* dan *script*. Umumnya pemberitahuan berisi data-data penjelasan tentang hal-hal dasar yang terjadi. Informasi yang lebih spesifik dikumpulkan dalam *reports*.

Jumlah pemberitahuan yang dikirim oleh sistem sangat tergantung seberapa kuat level yang dipasang. Semakin kuat level keamanan yang dipasang maka semakin banyak pemberitahuan yang dikirimkan. Ketelitian pemasangan level keamanan akan sedikit banyak membantu menurunkan jumlah pemberitahuan, dan hanya pemberitahuan tentang gangguan keamanan tertentu saja yang dikirimkan.

5. Melaksanakan peraturan

Manajemen keamanan informasi yang baik adalah kunci terlaksananya peraturan/regulasi yang dibuat. Dan itu adalah salah satu alasan pentingnya penerapan IDPS, terutama di organisasi yang menjalankan regulasi dengan ketat seperti institusi keuangan atau perusahaan kesehatan.

Dengan menerapkan IDPS, sebuah perusahaan dapat mempertahankan akuntabilitasnya, memberikan kejelasan hak akses kepada *user* dan memberikan dukungan infrastuktur yang tepat.

6. Menggalakkan kebijakan keamanan jaringan

Peralatan IDPS tidak hanya melindungi sistem dari penyusup yang bermaksud jahat, tetapi juga melindungi gangguan yang disebabkan oleh kesalahan operasional user atau dari pembalasan dendam karyawan yang frustrasi. Dari pengalaman perusahaan-perusahaan dalam beberapa tahun belakangan ini, gangguan keamanan sistem yang disebabkan oleh orang dalam ternyata cukup signifikan.

IDPS dapat dikonfigurasi sebagai alat untuk mengidentifikasi pelanggaran kebijakan keamanan dengan menset-nya seperti sebuah firewall. Juga dapat diset untuk memantau pengunaan akses yang tidak tepat seperti mentransfer file secara ilegal.

Setting pemantauan user ini perlu diumumkan kepada para users, agar para users mengetahui bahwa setiap penggunaan akses akan dipantau. Hal ini diharapkan meminimalisir keinginan/usaha penyalahgunaan hak akses.

Selain itu IDPS juga dapat menolong administrator untuk memelihara dan mempertajam kebijakan keamanannya. Sebagai contoh, IDPS akan memberitahu administrator jika didalam jaringan terdapat duplikasi setting firewall atau menangkap trafik mencurigakan yang lolos dari firewall.

7. Membatasi *chatting* (IM) dan video s*treaming* non-bisnis

Chatting atau IM (*instant messaging*) dan video *streaming* saat ini telah menjadi sebuah gaya hidup, baik urusan pribadi maupun urusan pekerjaan. Sehingga melarang aktifitas *chatting* dan video *streaming* dalam perusahaan bukanlah solusi terbaik. Namun penggunaan aktifitas tersebut yang tidak terkendali tentunya akan menghabiskan sumber daya perusahaan secara sia-sia.

Perusahaan dapat memanfaatkan IDPS untuk menjamin penggunaan sarana internet tersebut agar lebih banyak digunakan bagi kepentingan pekerjaan. Ini merupakan fungsi unik dari IDPS, proactive bussiness policy-setting device.

Perlu diwaspadai bahaya yang mungkin terjadi saat pertukaran informasi melalui IM. Yaitu saat terjadi pertukaran file attachment yang disisipi program jahat (malware) seperti worm. Sekali worm itu masuk kedalam sistem, maka penyerang akan dapat menggunakannya untuk masuk ke host jaringan komputer dan mengambil keuntungan dari akses yang telah diperolehnya tersebut. Beberapa peralatan IDPS telah dapat digunakan untuk

menghentikan dan mencegah penyisipan malware ini.

8. Lebih memahami aktifitas dalam network

IDPS mencatat semua lalulintas informasi dalam jaringan, termasuk bila ada hal yang mencurigakan yang telah berhasil menyusup kedalam sistem. Catatan ini memiliki dua kegunaan : (1) staf TI lebih memahami kemampuan peralatan IDPS ini sebelum alat itu menjadi bagian aktif dalam perusahaan; (2) memberikan pengetahuan dasar tentang berbagai macam data yang masuk dan keluar dari jaringan setiap hari.

Kedua hal itu berguna ketika staf TI akan mengambil sebuah keputusan operasional untuk melindungi aset-aset perusahaan. Dan juga memberikan pengalaman nyata kepada para eksekutif perusahaan tentang berbagai macam ancaman yang mencoba masuk.

9. Menghemat waktu

Dengan IDPS, staf TI tidak perlu menyisir secara manual *log* dalam *firewall* setiap hari yang akan memakan waktu sangat lama. Juga mencegah terjadinya kelumpuhan jaringan yang diakibatkan oleh serangan. Tentunya bila jaringan sempat lumpuh membutuhkan waktu yang lama untuk memulihkannya.

10. Memantau program aplikasi yang diinstal user

Peralatan IDPS dapat menolong staf TI menemukan aplikasi yang di download oleh user dalam jaringan. Jika aplikasi tersebut diperkirakan dapat merusak sistem, staf TI dapat dengan segera mencegahnya.

11. Membangun kepercayaan

IDPS tidak hanya menurunkan risiko keamanan jaringan perusahaan, tetapi juga memberikan keyakinan bahwa sistem tersebut aman dari serangan program-program jahat serta tidak berpotensi menyebarkannya kepada jaringan milik mitra bisnis.

12. Menghemat biaya

IDPS dapat menghemat biaya yang terjadi akibat kelumpuhan sistem, biaya teknisi untuk penelusuran *malware* secara manual setiap hari, dan pemborosan biaya-biaya lain akibat kerusakan sistem yang tidak perlu. Dan tentunya biaya kepercayaan dari mitra bisnis yang tidak dapat dihitung secara eksak.

3.4. Perbedaan IPS dan IDS

Ada perbedaan yang mendasar antara Intrusion Detection System (IDS) dan IPS menurut Rainer Bye (2009) seperti pada tabel dibawah ini :

Tabel 1 : Perbedaan IPS dan IDS

	IDS	**IPS**
OSI Layer	Layer 3	Layer 2, 3 dan 7
Kegunaan	IDS didesain hanya untuk mengidentifikasi dan memeriksa semua paket yang lewat, jika ditemukan keganjilan maka akan mentrigger alarm	Mengkombinasikan Firewall, Policy, QoS dan IDS dengan baik. IPS memang dibuat untuk dapat mentrigger alarm dan melakukan Allow, Block, Log
Aktivitas	Mendeteksi serangan hanya disaat serangan tersebut telah masuk ke jaringan dan tidak akan melakukan sesuatu untuk menghentikannya	Early Detection, teknik yang proaktif, mencegah sedini mungkin attack masuk ke jaringan, dan akan menghentikannya jika teridentifikasi
Komponen	Tidak dapat mendeteksi semua aktivitas malicious dan malware setiap saat yang akan mengakibatkan false negative sangat banyak	Memungkinkan dapat mendeteksi new signature dan behavior attack,dan mengakibatkan rendahnya false negative
Integrated	Tidak dapat menggunakan ACL / script dari komponen system keamanan yang lain	Dapat diintegrasikan dengan ACL dan perimeter DMZ lainnya

IPS (Intrusion Prevention System) merupakan jenis metode pengamanan jaringan baik software atau hardware yang dapat memonitor aktivitas yang tidak diinginkan atau intrusion dan dapat langsung bereaksi untuk untuk mencegah aktivitas tersebut. IPS (Intrusion Prevention System) merupakan pengembangan dari dari IDS (Intrusion Detection System) .Sebagai pengembangann dari teknologi firewall, IPS melakukan kontrol dari suatu sistem berdasarkan aplikasi konten atau pattern, tidak hanya berdasarkan ports atau IP address seperti firewall umumnya. .

Intrusion Detection System selain dapat memantau dan monitoring, IPS (Intrusion Prevention System) dapat juga mengambil kebijakan dengan memblock paket yang lewat dengan cara 'melapor' ke firewall.

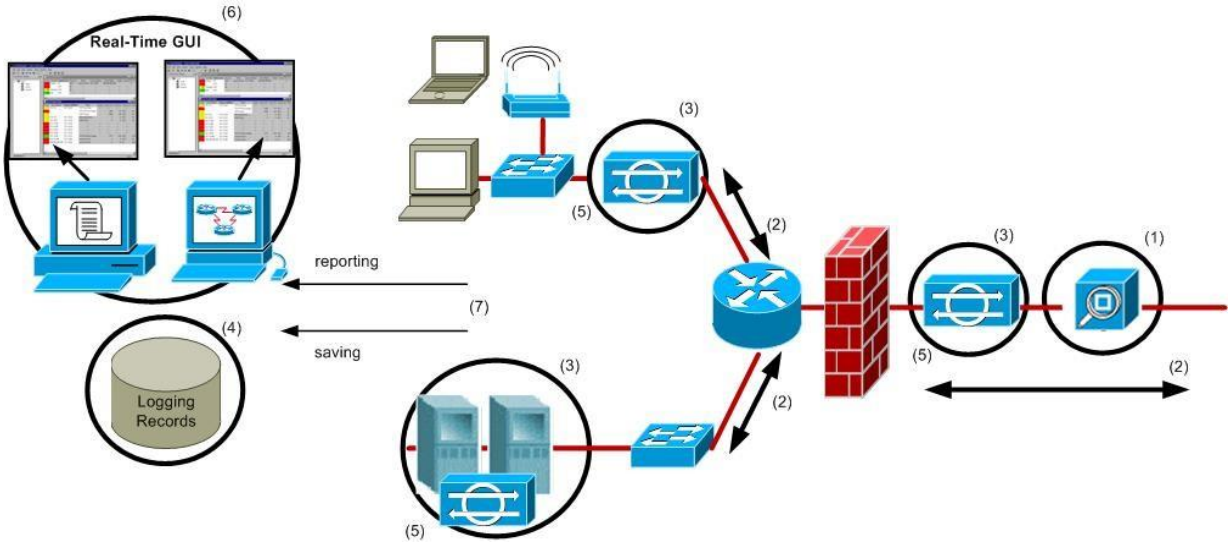
3.5. Implementasi IPS Dalam Mengamankan Komputer

Seiring dengan berkembangnya teknologi mengenai jaringan komputer, maka berkembang pula metode pengamanannya. Hal ini dikarenakan agar keamanan dari informasi di dalam jaringan tersebut dan juga keamanan jaringan itu sendiri dapat terjaga keamanannya dari para punyusup atau intruder. Karena hal tersebutlah diperlukan metode keamanan berupa pendeteksian dan pencegahan, metode tersebut terdapat di dalam IDS (Intrusion Detection System) dan IPS (Intrusion Prevention System) yang dapat melakukan pengaturan agar keamanan Informasi dalam jaringan tersebut dapat di manage atau dijaga dan juga keamanan jaringannya pun menjadi lebih secure atau aman.

IPS (Intrusion Prevention System) adalah sebuah metode pengamanan jaringan yang dapat berupa software ataupun hardware. IPS dapat melakukan monitoring terhadap seluruh aktifitas pada jaringan, IPS akan langsung melakukan pencegahan terhadap gangguan – gangguan atau intrusion seperti blocking atau drop program gannguan.

Kelebihan dari IPS adalah sistem yang dimilikinya, IPS memilki kecerdasan buatan sendiri yang dapat mempelajari dan mengenali serangan dan metode yang digunakan dalam penyerangan tersebut (TRIGER). IDS (Intrusion Detection System) dan IPS (Intrusion Prevention System) melakukan pendeteksian dan pencegahan terhadap gangguan atau intrusion berdasarkan signature atau pattern yang terdapat pada rule yang dibuat. Paket data yang datang terlebih dahulu akan di periksa kecocokannya terhadap rule yang dibuat, apabila terdapat kesamaan pada rule yang maka secara otomatis IDS (Intrusion Detection System) dan IPS (Intrusion Prevention System) akan melakukan peringatan (allert) dan selanjutnya akan melakukan pencegahan berupa blocking terhadap gangguan tersebut.

3.6. Topologi IPS



Gambar 3. Topologi dan terminologi dalam implementasi IPS (Deris S., A. Hanan, M. Yazid, 2010)

Berikut ini adalah beberapa istilah atau terminologi yang digunakan dalam mengimplentasikan Topologi IPS :

1. Akurasi Signature

Keakurasian signature sangat ditentukan oleh sensor dan update informasi yang ada, dimana sensor membuat alert, disuatu kondisi mentrigger alarm dari sensor (valid atau tidak), jika tidak valid terdeteksi bisa juga sangat memungkinkan sebagai serangan. Ada empat alert yang dibuat oleh sensor, seperti (i) True Negative (TN) : dimana pada kondisi traffic normal dan tidak ada alarm yang dibangkitkan, (ii) True Positive (TP) akan mentrigger alarm jika ditemukan kecocokan yang diidentifikasi sebagai serangan, (iii) False Negative (FN) akan tetap diam dengan tidak memberikan alarm walaupun attack telah masuk dan menyerang, dan (iv) False Positive (FP) membuat alert pada kondisi aktivitas traffic normal, fokus utama banyak peneliti adalah pada bagaimana untuk mengurangi alert FP ini. IPS seperti memiliki hidung dan

mata untuk mengidentifikasi semua data paket inbound-outbound.

2. Volume Traffic

Volume traffic sangat dipengaruhi oleh perangkat yang digunakan. Hal ini akan meningkat dengan tingginya traffic jaringan yang akan dipantau, yang akan mempengaruhi performance secara keseluruhan. Dibutuhkan klarifikasi jumlah paket traffic yang digunakan. Jumlah keseluruhan traffic didapat dari jumlah segment jaringan dan jumlah sensor yang ditempatkan. Penggunaan Fast Eth dan Gigabit Eth akan mempengaruhi dari faktor ini. Hubungannya adalah akan mempengaruhi kinerja jaringan secara keseluruhan. Hal ini penting karena setiap node jaringan dapat membuat permasalahan, termasuk kesalahan hardware, laporan kesalahan sistem operasi, perangkat jaringan akan menghasilkan broadcast yang memerlukan bandwidth.

3. Topologi Penempatan Sensor

Dalam sesi ini, harus diidentifikasi akses yang akan dibuat, misalnya akses juga akan diberikan ke mitra bisnis, dan koneksi dapat di lakukan telecommutes secara mobile. Tujuannya adalah untuk menentukan model aksesnya. Terdapat dua akses, yaitu akses outside dan inside, akses outside langsung terhubung ke Internet, sedangkan inside adalah sisi jaringan yang terpercaya. Sedangkan DMZ adalah dari sisi perimeter demiliterisasi zone, untuk mengidentifikasi dan memonitoring server farm. Terdapat dua faktor yang akan mempengaruhi dalam hal ini, (i) penempatan sensor, dan (ii) jumlah sensor yang akan digunakan. Kejelian dalam menentukan dua faktor ini akan meningkatkan akurasi dalam pengenalan pola serangan yang akan dilakukan.

Penempatan disisi outside akan memonitor dan mengidentifikasi paket yang akan masuk dan keluar, sedangkan penempatan di sisi inside misalnya di core, distribution atau access akan mempengaruhi keakuratan yang

dimonitor, karena sifat sensor ini hanya akan mengidentifikasi paket yang lewat di interfacenya.

4. Penggunaan Quota Log

Pada penelitian sebelumnya, semua system logs disimpan pada peralatan yang aman, model dengan menggunakan redundancy ditawarkan dengan jaminan high reliability yang tinggi (Taras Dutkevych, 2007). Namun tidak menjelaskan secara detail secara teknis bagaimana konfigurasi secara teknis dan peralatan yang digunakan. Hal ini berkaitan dengan berapa besar penggunaan media storages yang akan digunakan, dalam pantauan yang dilakukan dalam jaringan sesungguhnya yang dilakukan, pada percobaan yang dilakukan, didapat log sebesar 150 MBps di traffic jaringan dengan bandwidth ke internasional 135 Mbps. Sedangkan pengambilan data hanya data transaction (IP Add dan Mac Add) bukan dataset secara utuh.

Pada isu permasalahan ini, ada banyak sekali log file yang didapat dari logging system, seperti transaksi data log, log data attack, log data traffic, log record insiden, log notifikasi insiden, log laporan kegagalan, dan sebagainya yang memerlukan media storage yang besar.

5. Proteksi Mesin IPS

Terdapat beberapa statement dan kesimpulan penelitian sebelumnya, dimana Xinyau Zhang (2007) membuat intrusion prevention dengan berbasis SNMP untuk mengintegrasikan dengan system pertahanan yang lain, sedangkan Anh Le (2008) mengatakan implementasi load balancing dengan menggunakan libcap library dengan teknik clustering. Namun sangat disayangkan, tidak ada yang membahas tentang bagaimana menjaga mesin IPS dari serangan yang mungkin akan dilakukan penyerang. Dalam pengamatan sangat dimungkinkan penyerang akan

menyerang IPS. Dari sisi penyerang, hacker akan melakukan serangan pada mesin target dengan berbagai cara dan mekanisme, dimana serangan akan direncanakan dengan baik. Ada beberapa tahapan secara umum seperti : probe, scan, intrusion dan goal (Zhijie Liu, 2008). Menurut pengamatan yang dilakukan terdapat banyak cara penyerang untuk mencari kelemahan, langkah scanning yang sering dilakukan untuk mencari titik kelemahan tersebut, baik yang hanya sekedar mengumpulkan informasi seperti IP Address, skema diagram, aplikasi yang dijalankan, model firewall yang diintegrasikan sampai dengan mencari celah user dan password.

6. Sensor Monitoring

Sensor merupakan bagian kritikal di IPS, namun sangat disayangkan, capacity sensor ini sangat dibatasi oleh jumlah dari trafik jaringan, penempatan sensor, dan penggunaan system (apakah hardware atau berbasis module), karenanya solusi SPAN (Switched Port Analyzer) dapat digunakan untuk mengidentifikasi dan mengenali paket-paket tersebut.

Sensor monitoring digunakan untuk mengintegrasikan dan mencakup infrastruktur keamanan yang tersebar agar bisa berinteraksi secara dinamis dan otomatis dengan perangkat keamanan yang berbeda. Berarti disini dibutuhkan suatu mekanisme system monitoring yang terpadu (Sourour M., 2008).

7. Kolaborasi U.T.M

Pada sesi ini, kolaborasi system keamanan akan menjadi fokus utama. Unified Threat Management (UTM) coba ditawarkan disesi ini. Ada beberapa model dalam system keamanan ini, namun sangat disayangkan, model-model ini biasanya mempunyai standar sendiri-sendiri yang tidak dapat diintegrasikan satu dengan yang lain. Dalam pengamatan yang dilakukan terdapat tiga bagian utama pada system

keamanan computer, (i) web security, (ii) network protection, and (iii) mail filtering.

4. Kesimpulan

Dari pembahasan dapat disimpulkan bahwa :

a) IPS (Intrusion Prevention System) digambarkan seolah – olah bekerja pada bagian luar network dan mendeteksi seluruh paket data yang datang untuk kemudian akan di analisa apakah paket data tersebut berupa gangguan atau intrusi dengan mencocokkan signature atau pattern paket data tersebut dengan rule yang dibuat.
b) Sangat penting untuk melakukan manajemen Keamanan informasi. Untuk melakukannya tidak hanya butuh satu metode keamanan yang sangat baik, tetapi akan lebih baik dan dibutuhkan beberapa metode keamanan yang saling bekerja sama untuk menutupi kekurangannya karena selama masih dalam konteks buatan manusia, metode keamanan tersebut tidak akan sempurna.
c) Kemanan komputer merupakan aspek yang sangat vital ketika komputer yang digunakan tersebut terhubung dalam jaringan baik lokal maupun global. Untuk mencegah penyusupan maka diperlukan sebuah sarana yang digunakan untuk mendeteksi dan mencegahnya. IPS adalah solusi dari tindak pencegahan intrusi masuk ke dalam komputer kita.

Daftar Pustaka

Anh Le, et al, 2008, ” *On Optimizing Load Balancing of Intrusion Prevention and Prevention Systems*”, IEEE, INFOCOM Workshops.

Deris S., A. Hanan, M. Yazid, 2010, “*The Measurement Internet Services*”, International Conferences, ICGC-RCICT.

E. Carter, et al, 2006, “*Intrusion Prevention Fundamentals : an introduction to*

network attack mitigation with IPS", Cisco press.

Rainer Bye, et al, 2009, "*Design and Modeling of Collaboration Architecture for Security*", International Symposium Collaborative Technologies and Systems.

Robert Richardson, 2008, "*CSI Computer Crime & Security Survey 2008*".

Sourour M., et al, 2008, "*Collaboration between Security Devices toward improving Network Defense*", sevent IEEE/ACIS International Conference on Computer and Information Science.

Sundaram, A., 1996, "*An Introduction to Intrusion Detection"*, USA: Whitepaper.

Taras Dutkevych, et al, 2007, "*Real-Time Intrusion Prevention and Anomaly Analyze System for Corporate Networks*", IEEE International Workshop on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications.

Wardhani, H. M., 2010, "*Intrusion Detection System*", http://helenamayawardhani.wordpress.com

Wirartha, I.M., 2006, "Metodologi Penelitian Sosial Ekonomi", Yogyakarta, Penerbit Andi.

Xinyau Zhang, et al, 2004, "*Intrusion Prevention System Design*", Computer and Information Technology.

Zhijie Liu, et al, 2008, "*Correlating Multi-Step Attack and Constructing Attack*

Scenarios Based on Attack Pattern Modeling“, International Conference on Information Security and Assurance.