p-ISSN 1693-9484, *e*-ISSN : 2621-8313
Majalah Ilmiah Bahari Jogja (MIBJ)
Vol. 17 No. 2, Juli 2019 (1-9)
DOI : 10.33489/mibj.v17i2.205

Implementasi *Network Intrusion Detection System* (NIDS) Dalam Sistem Keamanan Open Cloud Computing

Muqorobin[1*], Zul Hisyam[1], Moch. Mashuri[1], Hanafi[1], Yudhi Setiyantara[2]
[1]Universitas Amikom Yogyakarta, Jl. Ring Road Utara, Condong Catur, Sleman, Yogyakarta, Indonesia
[2]Akademi Maritim Yogyakarta, Jl. Magelang KM 4.4, Sinduadi, Mlati, Sleman, Yogyakarta 55284, Indonesia
* Corresponding Author. E-mail: robbyaullah@gmail.com. Telp:+6285702302019

Abstrak

Keamanan merupakan bagian terpenting dalam sistem teknologi jaringan komputer. Diantara teknologi yang memanfaatkan jaringan adalah *cloud computing*. Salah satu penyedia *cloud computing* seperti *eucalyptus* menggunakan *firewall* untuk keamanan sistem. Penggunaan *firewall* pada sistem tidak dapat memantau dan menganalisa *traffic* yang berada di dalam server *cloud* dan tidak memberikan peringatan ketika terjadi sebuah serangan. Tujuan dari penelitian ini adalah peneliti akan menerapkan sebuah *network intrusion detection system* (NIDS) dilingkungan *cloud computing* dan *mirroring traffic* pada switch. *Intrusion detection system* (IDS) merupakan suatu teknologi keamanan yang mampu menganalisis *traffic* jaringan dan mendeteksi *traffic* apabila terindikasi serangan. NIDS ditempatkan dihost yang berbeda dengan server *cloud computing*. Dengan metode *mirroring traffic* pada switch, *traffic* akan diarahkan ke NIDS sehingga NIDS mampu merekam semua *traffic* jaringan yang berasal dari luar server *cloud* ataupun *traffic* antar *virtual machine* di dalam server *cloud*. Hasil pengujian serangan dengan 2 skenario yaitu penyerangan dari luar dan dari dalam sistem *cloud*, maka NIDS mampu memberikan respon alert untuk *traffic* serangan.
Kata Kunci : Cloud Computing, NIDS, Mirroring Traffic, firewall.

Abstract

Security is the most important part of computer network technology systems. Among the technologies that utilize networks are cloud computing. One cloud computing provider such as eucalyptus uses a firewall for system security. The use of a firewall on the system cannot monitor and analyze traffic that is inside the cloud server and does not give a warning when an attack occurs. The purpose of this study is that researchers will implement a network intrusion detection system (NIDS) in cloud computing and mirroring traffic on switches. Intrusion detection system (IDS) is a security technology that can analyze network traffic and detect traffic if an attack is indicated. NIDS are placed hosted differently from cloud computing servers. With the switch mirroring traffic method, traffic will be directed to NIDS so that NIDS can record all network traffic originating from outside the cloud server or traffic between virtual machines within the cloud server. The test results of attacks with 2 scenarios, namely attacks from outside and from within the cloud system, then NIDS is able to provide an alert response to traffic attacks.

Keywords: Cloud Computing, NIDS, Mirroring Traffic, firewall.

PENDAHULUAN

Cloud Computing adalah teknologi komputasi yang menggunakan layanan internet dalam mengakses *resources. Infrastructure as a Service* (IaaS) merupakan salah satu layanan *cloud computing* yang menyewakan infrastruktur IT berupa *storage, networks* dan sumber daya komputasi lainnya. Berdasarkan survey yang dilakukan oleh *International Data Corporation* (IDC) menunjukkan bahwa keamanan merupakan tantangan dalam teknologi *cloud computing*. Selain itu salah satu masalah keamanan yang utama dalam *cloud computing* adalah melindungi infrastruktur yang terdapat di dalamnya dari serangan jaringan. Infrastruktur *cloud computing* yang mengadopsi teknologi virtualisasi memungkinkan penyusup untuk memanfaatkan *vulnerabilities* yang tersedia. Teknologi *cloud computing* juga mengalami beberapa *traditional attack* yang biasanya terdapat pada jaringan secara umum seperti *IP Spoofing, DNS Poisoning, Flooding dan Distributed Denial of Service* (DDoS).

Network Intrusion Detection System (NIDS) merupakan salah satu IDS yang ditempatkan di salah satu titik sebuah jaringan dan berfungsi untuk memantau serta menganalisis lalu lintas paket data dalam jaringan. Dengan menggunakan IDS berbasis *network*, letak IDS dalam *cloud* berada di *external network* atau di dalam *virtual network*. Sehingga memiliki keterbatasan dalam mendeteksi serangan di dalam *virtual network*.

Dalam penelitian ini, penulis mengusulkan *Intrusion Detection System* berbasis jaringan (NIDS) untuk layanan *Infrastrukture as a Service* (IaaS) yang diimplementasikan pada *open* c*loud computing*. Dengan menggunakan *mirroring*pada switch, *traffic* akan diarahkan ke NIDS sehingga NIDS mampu memantau semua *traffic* jaringan yang berasal dari luar server *cloud* maupun *traffic* yang ada antar *virtual machine* di dalam server *cloud*. Tugas utamanya adalah memantau aktivitas yang mencurigakan dari luar c*loud computing* dan antar host di dalam c*loud computing* dan memberikan laporan ke administrator jaringan jika ada serangan yang terjadi di lingkungan sistem(Ali, Venus, & Rababaa, 2009).

Intrusion Detection System (IDS)

IDS adalah sebuah aplikasi perangkat keras atau perangkat lunak yang otomatis bekerja untuk memonitor kejadian pada sebuah jaringan komputer dan sekaligus menganalisais masalah keamanan jaringan. Sasaran *IDS* adalah memonitoring aset jaringan sehingga dapat mendeteksi perilaku yang tidak lazim, kegiatan yang tidak sesuai, searngan atau menghentikan serangan (penyusupan) dan bahkan menyediakan informasi untuk menelusuri penyerang. Pada umumnya *IDS* terbentuk menjadi dua, yaitu (Ulfa, 2013).

1. *Network-Based Intrusion Detection System (NIDS). NIDS* merupakan strategi yang efektif untuk melihat *traffic* masuk keluar ataupun *traffic* di antara *host* atau di antara segmen jaringan lokal. *NIDS* biasanya dikembangkan di depan dan di belakang *firewall* dan VPN *gateway* untuk mengukur keefetifan peranti-peranti keamanan tersebut dan berinteraksi dengan mereka untuk memperkuat keamanan jaringan.
2. *Host-Based Intrusion Detection System (HIDS)*. *HIDS* hanya melakukan pemantauan pada perangkat komputer tertentu dalam jaringan *HIDS* biasanya

akan memantau kejadian seperti kesalahan login berkali-kali dan melakukan pengecekan pada file.

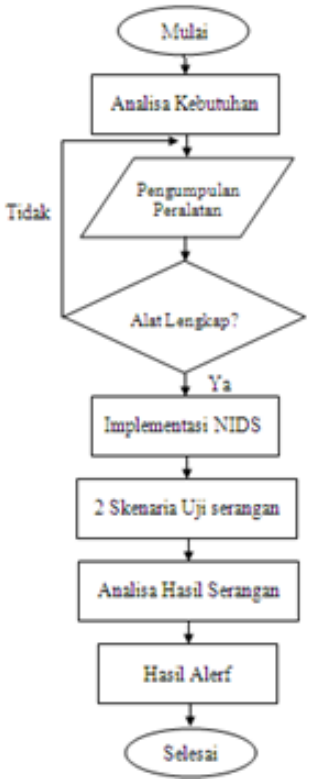
Cloud Computing

Cloud Computing sendiri bisa berarti akses fasilitas komputer secara bersama-sama melalui Internet dari berbagai lokasi (Ashari Setiawan, 2011). *Cloud Computing* memiliki 5 karakteristik yang penting, yaitu :

1. *On-deman self-service.* Konsumen dapat menentukan kemampuan komputasi secara sepihak, seperti *server time* dan *network storage*, secara otomatis sesuai kebutuhan tanpa memerlukan interaksi manusia dengan masing-masing penyedia layanan.
2. *Broad network access*. Kemampuan yang tersedia melalui jaringan dan diakses melalui mekanisme standar yang mengenalkan penggunaan berbagai platform (misalnya, telepon selular, tablets, laptops, dan workstations).
3. *Resource pooling*. Penyatuan sumber daya komputasi yang dimiliki penyedia untuk melayani beberapa konsumen virtual yang berbeda, ditetapkan secara dinamis dan ditugaskan sesuai dengan permintaan konsumen. Ada rasa kemandirian lokasi bahwa pelanggan pada umumnya tidak memiliki control atau pengetahuan atas keberadaan lokasi sumberdaya yang disediakan, tetapi ada kemungkinan dapat menentukan lokasi di tingkat yang lebih tinggi (misalnya, negara, negara bagian, atau data center). Contoh sumberdaya termasuk penyimpanan, pemrosesan, memori, bandwidth jaringan, dan mesin virtual.
4. *Rapid elasticity*. Kemampuan dapat ditetapkan dan dirilis secara elastis, dalam beberapa kasus dilakukan secara otomatis untuk menghitung keluar dan masuk dengan cepat sesuai dengan permintaan. Untuk konsumen, kemampuan yang tersedia yang sering kali tidak terbatas dan kuantitasnya dapat disesuaikan setiap saat.
5. *Measured Service. Sistem cloud computing* secara otomatis mengawasi dan mengoptimalkan penggunaan sumberdaya dengan memanfaatkan kemampuan pengukuran (metering) pada beberapa tingkat yang sesuai dengan jenis layanan (misalnya, penyimpanan, pemrosesan, bandwidth, dan account penggunaaktif). Penggunaan sumber daya dapat dipantau, dikendalikan, dan dilaporkan sebagai upaya memberikan transparansi bagi penyedia dan konsumen dari layanan yang digunakan.

METODE

Metode penelitian yang digunakan dalam Impelementasi *Network-Based Intrusion Detection System* (NIDS) dengan metode observasi yaitu dengan menganalisa terhadap sistem serta aspek-aspek lain yang dapat mempengaruhi terhadap jalannya sistem baik dari sisi lingkungan maupun dari sisi pengguna sistem itu sendiri. Selain itu, peneliti juga menggunakan Metode *study* kepustakaan yang dilakukan untuk menunjang metode observasi yang telah dilakukan. Pengumpulan informasi yang dibutuhkan dilakukan dengan mencari referensi-referensi yang berhubungan dengan penelitian yang dilakukan, referensi dapat diperoleh dari buku-buku atau internet. Untuk gambaran alur penelitian dapat dilihat pada Gambar 1 sebagai berikut :



Gambar 1. Alur Penelitian

Adapun penjelasan dari tahapan alur penelitian sebagai berikut :

a. Tahap ke 1 yaitu analisis kebutuhan, Pada tahap ini peneliti menganalisa berbagai kebutuhan yang dibutuhkan dalam melakukan penelitian dan juga membuat daftar kebutuhan sistem dan aplikasi pendukung lainnya.
b. Tahap ke 2 pengumpulan peralatan peneliti mulai mencari dan mengumpulkan perlengkapan dan peralatan yang dibutuhkan seperti software maupun hardware yang berkaitan dengan masalah penelitian.
c. Tahap ke 3 instalasi sistem Dalam hal ini dimulai dengan menginstal sistem operasi yang akan digunakan sebagai IDS sampai dengan mengatur konfigurasi sistem dan jaringan agar dapat berjalan dengan baik.
d. Tahap ke 4 skenario pengujian NIDS, Peneliti membuat skenario atau rencana pengujian pada sistem. Dalam hal ini peneliti membuat skenario serangan yang ditujukan kepada sistem. Kemudian melakukan uji coba terhadap sistem yang telah dipersiapkan dengan mempraktikan skenario penyerangan yang sudah dibuat.
e. Tahap ke 5 analisa hasil pengukuran Menganalisa hasil pengukuran kinerja NIDS yang diperoleh dari data serangan atau alert yang dihasilkan oleh sistem NIDS.

f. Tahap ke 6 yaitu laporan Penulis membuat laporan dari hasil penelitian yang sudah dilakukan.

HASIL DAN PEMBAHASAN

Keamanan Data Pada *Cloud Computing* (*Data Security on Cloud Computing*) sangatlah penting sekaligus masih menjadi tantangan bagi beberapa orang untuk meningkatkan kualitas keamanan jaringan Cloud computingdimana berbagai data di dalamnya bisa saja dicuri atau diintip oleh pihak-pihak tidak bertanggung jawab.

Dalam jurnal ini, peneliti mengusung metode IDS sebagai alternatif lain dalam memproteksi data pada sistem komputasi awan. Peneliti mengusulkan *Intrusion Detection System* berbasis jaringan (NIDS) untuk layanan *Infrastrukture as a Service* (IaaS). Dengan menggunakan *mirroring* pada switch, *traffic* akan diarahkan ke NIDS sehingga NIDS mampu memantau semua *traffic* jaringan yang berasal dari luar server *cloud* maupun *traffic* yang ada antar *virtual machine* di dalam server *cloud* (Barbosa Pras, 2010).

Untuk membuktikan keampuhan metode ini, penulis melakukan 2 pengujian yaitu pengujian penempatan NIDS dan pengujian serangan. Pengujian penempatan NIDS dilakukan untuk mengetahui apakah penempatan NIDS yang berbeda host dengan server *cloud* mampu menangkap dan merekam *traffic* yang berasal dari luar sistem dan *traffic* di dalam sistem server *cloud*. Selanjutnya pengujian dilanjutkan dengan pengujian serangan secara langsung untuk membuktikan apakah penempatan NIDS mampu untuk mendeteksi serangan (Bellettini Rrushi, 2008).

Pengujian penempatan NIDS dilakukan dengan cara melakukan komunikasi antar *virtual machine* dalam server *cloud* dan komunikasi dari luar server dengan salah satu *virtual machine*. Kemudian menguji apakah NIDS mampu menangkap dan merekam *traffic* tersebut dengan metode *mirroring traffic* pada switch.

Untuk pengujian penempatan nids dari luar sistem, NIDS telah mampu menangkap dan merekam *traffic* dari luar sistem, hal ini menunjukkan *mirroring traffic* untuk komunikasi dari luar sistem telah berhasil. Sementara untuk Pengujian penempatan NIDS dari dalam sistem, NIDS juga mampu menangkap komunikasi antar *virtual machine* di dalam server *cloud*. Hal ini menunjukkan bahwa *mirroring traffic* yang dilakukan pada sistem ini telah berhasil(Bastani & Houston, 1994).

Pengujian serangan dilakukan dengan cara melakukan serangan ke dalam jaringan untuk melihat kemampuan sistem dalam mendeteksi penyerangan yang ada. Untuk pengujiandari luar sistem dan dalam sistem, alert berhasil memberikan peringatan namun pada bagian tertentu gagal mendeskripsikan bentuk serangan.

Untuk melakukan pengujian pada sistem ini, dilakukan 2 pengujian, yaitu pengujian penempatan NIDS dan pengujian serangan. Pengujian penempatan NIDS pada lingkungan *open cloud computing* dilakukan dengan maksud apakah penempatan NIDS yang berbeda host dengan server *cloud* mampu menangkap dan merekam *traffic* yang berasal dari luar sistem dan *traffic* di dalam sistem server *cloud* (Bao, Chen, Chang Cho, 2012).

Selanjutnya pengujian dilanjutkan dengan pengujian serangan secara langsung untuk membuktikan apakah penempatan NIDS mampu untuk mendeteksi serangan.

1. Pengujian Penempatan NIDS
   Pada pengujian ini, dilakukan pengaksesan virtual machine oleh komputer yang berada di luar sistem untuk menunjukkan apakah mirroring traffic dapat ditangkap dan direkam oleh NIDS. Dalam penelitian ini, NIDS telah mampu menangkap dan merekam traffic dari luar sistem, hal ini menunjukkan mirroring traffic untuk komunikasi dari luar sistem telah berhasil.
   a. Pengujian Penempatan NIDS Dari Luar Sistem
      Pada pengujian ini, dilakukan pengaksesan *virtual machine* oleh komputer yang berada di luar sistem untuk menunjukkan apakah *mirroring traffic* dapat ditangkap dan direkam oleh NIDS. Dalam penelitian ini, NIDS telah mampu menangkap dan merekam *traffic* dari luar sistem, hal ini menunjukkan *mirroring traffic* untuk komunikasi dari luar sistem telah berhasil.
   b. Pengujian Penempatan NIDS Dari Dalam Sistem
      Pada pengujian ini dilakukan komunikasi antar *virtual machine* di dalam server *cloud,* yang bertujuan untuk menunjukkan *traffic* di dalam server cloud dapat ditangkap dan direkam oleh NIDS. Vmbr0 yang sudah di setting menjadi mode *promiscuous* dan terhubung dengan eth1 ini akan mendengar komunikasi tersebut dan melakukan *mirroring traffic* pada switch menuju NIDS. Dalam penelitian ini, NIDS mampu menangkap komunikasi antar *virtual machine* di dalam server *cloud*. Hal ini menunjukkan bahwa *mirroring traffic* yang dilakukan pada sistem ini telah berhasil.
2. Pengujian Serangan
   Pengujian serangan dilakukan dengan cara melakukan serangan ke dalam jaringan untuk melihat kemampuan sistem dalam mendeteksi penyeranganyang ada. Pengujian ini dibagi menjadi dua, yaitu pengujian dari luar sistem dan pengujian dari dalam sistem.
   a. Pengujian Dari Luar Sistem
      Pada pengujian ini, sistem diserang oleh sebuah komputer attacker yang menyerang *virtual machine*. Serangan yang dilakukan adalah metasploit, Syn flood menggunakan Hping3 dan Scapy. Untuk hasil pengujian ditampilkan pada tabel 1 sebagai berikut :

Tabel 1. Data Hasil Pengujian dari Luas Sistem

Serangan	Alert	Keterangan
Detecting Vulnerable SSH Versions (Metasploit)	Snort Alert [1:13586:4]	Muncul Alert dan Terdeteksi Serangan
SSH Brute Force (Metasploit)	Snort Alert [1:13586:4]	Muncul Alert dan Terdeteksi Serangan
Attack Apache Server (Metasploit apache_mod_isapi)	Snort Alert [1:100000160:1]	Muncul Alert dan Terdeteksi Serangan
Synflood (Hping3)	Misc Source port 53 to < 1024	Muncul Alert dan Terdeteksi Serangan
Mengirim paket data menggunakan scapy	Misc Source port 20 to < 1024	Muncul Alert dan Terdeteksi Serangan

Ketiga alert diatas dihasilkan karena terjadi *non-legitimate traffic* yang melewati *firewall*(Bao et al., 2012).

b. Pengujian Dari Dalam Sistem

Pada pengujian ini Serangan dilakukan oleh komputer *virtual machine* (VM) kepada komputer *virtual machine* (VM)yang berada pada server proxmox. Pada pengujian ini dilakukan tujuh kali serangan terhadap VM. Dengan 3 kali *Port Scanning*, *SSH Brute Force* (Metasploit), *Attack Apache Server* (*Metasploit apachemodisapi*), *Synflood*(Hping) dan pengiriman paket data menggunakan scapy. Hasil pengujian dari dalam sistem ditampilkan pada tabel 2 berikut :

Tabel 2. Data Hasil Pengujian dari Dalam Sistem

Serangan	Alert	Keterangan
Port Scanning (Nmap Xmas scan)	Nmap Xmas scan	Muncul Alert dan Terdeteksi Serangan
Port Scanning (Nmap Connect())	• SNMP request tcp • SNMP trap tcp • SNMP AgentX/tcp request	Muncul Alert dan Terdeteksi Serangan
Port Scanning (full SYN scan)	• SNMP request tcp • SNMP trap tcp • SNMP AgentX/tcp request	Muncul Serangan dan Terdeteksi Serangan
Brute Force SSH Login (Metasploit)	SCAN SSH brute force login attempt	Muncul Serangan dan Terdeteksi Serangan
Attack Apache Server (Metasploit)	Snort Alert [1:19124:2]	Muncul Serangan dan Terdeteksi Serangan
Synflood (Hping3)	Misc Source port 53 to < 1024	Muncul Serangan dan Terdeteksi Serangan
Mengirim paket data	Misc Source port 20 to <	Muncul Serangan dan

Untuk serangan *port scanning* ada 3 macam *scanning* yang dilakukan, yaitu Port *Scanning* (Nmap Xmas scan), *Port Scanning* (Nmap Connect()) dan *Port Scanning* (full SYN scan).

SIMPULAN

Adapun Kesimpulan yang dapat penulis ambil dari serangkaian penelitian yang dilakukan dalam jurnal tersebut adalah :

1. Dengan penempatan NIDS yang terpisah dengan server *cloud* dan menggunakan VLAN switch untuk melakukan *mirroring traffic*, NIDS mampu menerima *traffic* yang menuju ke server maupun *traffic* antar *virtual machine* di dalam server *cloud*.
2. Hasil pengujian serangan secara langsung menggunakan 2 skenario, yaitu penyerang berada di luar sistem dan penyerang di dalam sistem *cloud*, NIDS mampu menerima *traffic*, menganalisis dan merespon serangan dengan menampilkan *alert*.
3. Untuk NIDS yang digunakan dalam sistem adalah IDS snort yang menggunakan *front-end* BASE. Penggunaan *front-end* pada NIDS mampu mempermudah administrator dalam memahami alert yang masuk.
4. Dengan penempatan NIDS yang berada di luar sistem *cloud computing*, membuat proses analisis *traffic* tidak mempengaruhi server *cloud computing*

DAFTAR PUSTAKA

Ali, K. M., Venus, W., & Rababaa, M. S. Al. (2009). The affect of fuzzification on neural networks intrusion detection system. *2009 4th IEEE Conference on Industrial Electronics and Applications, ICIEA 2009*, 1236–1241. https://doi.org/10.1109/ICIEA.2009.5138399

Ashari, A., & Setiawan, H. (2011). Cloud Computing : Solusi ICT ? *Jurnal Sistem Informasi (JSI)*, *VOL. 3*, *NO*, 336–345.

Bao, F., Chen, I. R., Chang, M. J., & Cho, J. H. (2012). Hierarchical trust management for wireless sensor networks and its applications to trust-based routing and intrusion detection. *IEEE Transactions on Network and Service Management*,*9*(2),169–183. https://doi.org/10.1109/TCOMM.2012.031912.110179

Barbosa, R. R. R., & Pras, A. (2010). Intrusion detection in SCADA networks. *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, *6155 LNCS*, 163–166. https://doi.org/10.1007/978-3-642-13986-4_23

Bastani, F. B., & Houston, H. (1994). Reliability of Systems with Fuzzy-Failure Criterion, 442–448. https://doi.org/10.1109/WCSP.2012.6542908

Bellettini, C., & Rrushi, J. L. (2008). A product machine model for anomaly detection of interposition attacks on cyber-physical systems. *IFIP International Federation for Information Processing*, *278*, 285–299. https://doi.org/10.1007/978-0-387-09699-5_19

Ulfa, M. (2013). Implementasi Intrusion Detection System (IDS) Di Jaringan Universitas Bina Darma. *Jurnal Ilmiah MATRIK*, *15*(12), 105–118. https://doi.org/10.1145/1809049.1809052