RANCANG BANGUN SISTEM PENCEGAHAN PENYUSUPAN PADA JARINGAN KOMPUTER BERBASIS CYBEROAM

Mufti Rizal
Bidang Pengembangan Sistem dan Jaringan dan Multimedia, Asdep Dukungan Data Kebijakan dan Informatika
Jl. Veteran No. 17-18 Jakarta Pusat 10110
E-mail: mufti.rizal@gmail.com

Abstrak
Peningkatan kebutuhan manusia terhadap teknologi informasi memicu meningkatnya kebutuhan sistem komputer dalam memenuhi kebutuhan dimaksud. Salah satunya adalah peningkatan penggunaan jaringan komputer, untuk menunjang kebutuhan yang meningkat terkadang mendorong penambahan perangkat jaringan komputer bahkan penambahan kapasitas bandwidth sebagai solusi tanpa memperhatikan lalu lintas data dan informasi pada jaringan komputer itu sendiri, sehingga menjadi percuma mengingat kenyataan yang terjadi yakni banyaknya penggunaan jaringan komputer untuk kebutuhan yang tidak diperlukan termasuk adanya penyusupan ke dalam jaringan komputer.

***Kata Kunci**: jaringan komputer, sistem pemantauan jaringan, manajemen log*

1. PENDAHULUAN

1.1. Latar Belakang Masalah

Semakin besar dan pentingnya pemanfaatan teknologi informasi dan komunikasi memicu meningkatnya kompleksitas sistem informasi yang harus dijaga demi mendukung kinerja secara keseluruhan. Salah satu sistem informasi yang memerlukan penanganan khusus adalah jaringan komputer sebagai urat nadi sistem komputer secara keseluruhan pada era teknologi informasi dan komunikasi seperti sekarang.

Banyak cara yang dilakukan dalam meningkatkan efektifitas dan performansi jaringan komputer antara lain menambah perangkat pendukung jaringan komputer serta meningkatkan kapasitas *bandwidth* sebagai penopang transaksi data dan informasi. Penambahan perangkat pendukung jaringan komputer serta meningkatkan kapasitas *bandwidth* ternyata tidak menjamin kehandalan transaksi data dan informasi dikarenakan banyak faktor yang harus diperhatikan dalam pengelolaan jaringan komputer. Disinilah dibutuhkan metode, inovasi dan terobosan-terobosan yang cerdas sehingga sistem informasi yang dibangun tidak menjadi percuma dan tidak tertinggal dengan yang lain.

Dalam memenuhi tuntutan yang tinggi terhadap ketersediaan jaringan komputer yang aman dan handal, sudah barang tentu tersedia perangkat *firewall* sebagai komponen utama keamanan sistem jaringan, tersedia berbagai jenis *firewall* baik yang bersifat *General Public License* maupun *proprietary*. Contohnya adalah Fortigate yang merupakan sebuah *firewall* yang bersifat *proprietary* yang tentunya memiliki banyak keunggulan dibandingkan dengan *firewall* yang bersifat gratis (*open source*), salah satu keunggulan dari *proprietary firewall* adalah tersedianya UTM (*Unified Threat Management*) untuk menjamin *QoS* performansi jaringan komputer.

Penggunaan *proprietary firewall* menjadi kurang efektif apabila tidak dilengkapi dengan perangkat yang juga *proprietary* untuk melakukan analisa lalu lintas data jaringan komputer, yang mana fungsi perangkat tersebut selain untuk menganalisa juga sebagai media penyimpan *log* lalu lintas data yang melewati *proprietary firewall*, harga perangkat *proprietary* yang sangat mahal menjadi kendala, sehingga tidak semuanya mampu menggunakan perangkat dimaksud.

1.2. Tujuan

Tujuan pembuatan makalah ini adalah membuat rancang bangun sistem pencegahan penyusupan pada jaringan komputer berbasis Cyberoam dengan melakukan analisa lalu lintas data pada jaringan komputer yang melewati *firewall*, sehingga diharapkan dapat memperkaya sistem pengamanan jaringan komputer dalam meningkatkan pelayanan dalam mengolah transaksi data dan informasi.

1.3. Ruang lingkup

Batasan makalah tentang rancang bangun sistem pencegahan penyusupan pada jaringan komputer berbasis Cyberoam ini adalah tentang analisa *event* lalu lintas data yang melalui jaringan komputer berdasarkan data *log* dari *Firewall* Fortigate menggunakan Cyberoam iView.

2. TINJAUAN PUSTAKA

2.1. Konsep Dasar Keamanan Sistem

Pengertian keamanan adalah selamat atau bebas dari segala resiko dan bahaya. Keamanan dalam jaringan komputer dikategorikan menjadi dua, yaitu keaman fisik dan non fisik. Keamanan fisik merupakan keamanan yang lebih cendering terfokus ke segala sesuatu yang bersifat fisik, jenis keamanan ini bisa dihindari

dengan cara lebih teliti menjaga secara fisik dari segala ancaman. Sedangkan keamanan non fisik berkaitan dengan nilai yang dimiliki, yang dapat menimbulkan permasalahan melebihi permasalahan fisik.

Keamanan jaringan komputer tidak bisa dilepaskan dari proses sistem informasi dan komunikasi. Secara tradisional ada tiga (3) unsur utama yang menjadi perhatian dalam keamanan sistem yang sering disebut dengan istilah CIA, yaitu :

1. Kerahasiaan (*confidentiality*), memastikan bahwa hanya pihak berwenang yang memiliki akses ke dalam data dan informasi;
2. Integritas (*integrity*), memastikan bahwa data dan informasi tidak dapat dimodifikasi oleh pihak yang tidak berhak sehingga dapat diandalkan;
3. Ketersediaan (a*vailability*), memastikan bahwa data dan informasi dapat diakses kapanpun saat dibutuhkan.

Pada tahapan selanjutnya 3 unsur diatas oleh oleh para praktisi keamanan sistem dijabarkan secara rinci kedalam beberapa hal, antara lain:

1. Otentikasi (a*uthentication*), metode untuk memastikan keaslian data dan informasi, pengguna atau sumber yang diakses;
2. Otorisasi/akses kontrol (a*uthorization/ access control*), untuk memastikan data dan informasi yang diakses sesuai dengan izin yang diberikan;
3. Dapat diaudit (a*uditability*), memastikan bahwa aktivitas dan transaksi pada sistem atau jaringan dapat dipantau dan tercatat untuk menjaga ketersediaan sistem dan mendeteksi penggunaan yang tidak sah;
4. *Nonrepudiation*, memastikan bahwa orang yang melakukan transaksi data dan informasi cukup otentik sehingga tidak dapat menyangkal telah melakukan transaksi.

2.2. SIEM (*Security Information Event Management)*

Istilah *Security Information Event Management* (SIEM) pertama kali dikemukakan oleh Mark Nicolett dan Amrit Williams pada tahun 2005, menggambarkan tentang kemampuan perangkat aplikasi untuk mengumpulkan, menganalisa dan menyajikan informasi tentang perangkat jaringan komputer beserta sistem keamanannya; identifikasi dan manajemen akses sistem komputer; manajemen celah keamanan sistem komputer dan *policy*; pencatatan *log* sistem operasi, *database* dan aplikasi; serta menyediakan data analisis ancaman yang berasal dari luar sistem.

Fokus utama dari SIEM adalah untuk memantau dan membantu pengelolaan layanan hak pengguna, layanan direktori serta menyediakan pencatatan *log auditing*.

2.3. *Firewall*

Firewall merupakan sistem atau perangkat yang mengizinkan transaksi komunikasi data melalui jalur lalu lintas pada jaringan komputer yang dianggap aman untuk melaluinya dan mencegah transaksi komunikasi data pada lalu lintas data jaringan komputer yang tidak aman, umumnya sebagai pintu gerbang (*gateway*) antara jaringan lokal dan jaringan komputer lainnya.

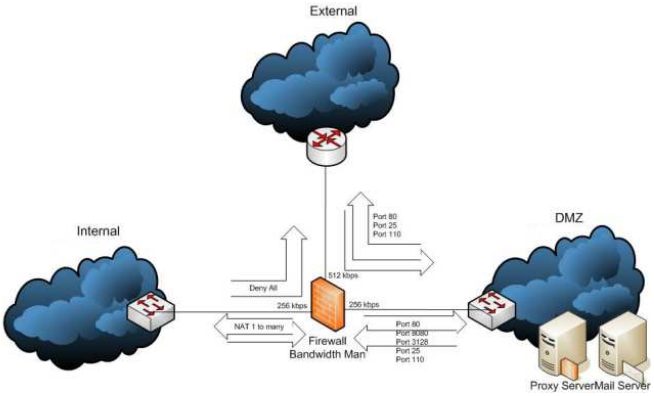
Fungsi lain *firewall* adalah untuk mengendalikan akses terhadap siapa saja yang memiliki akses terhadap jaringan pribadi dari pihak luar serta mengatur komunikasi antar dua sistem jaringan yang berbeda. Terdapat dua (2) jenis *firewall*, yaitu :

1. *Personal firewall,* aplikasi *firewall* yang didesain untuk melindungi sebuah komputer yang terhubung ke jaringan dari akses yang tidak dikehendaki;
2. *Network firewall, firewall* yang didesain untuk melindungi sistem jaringan komputer secara keseluruhan dari berbagai serangan. Umumnya dijumpai dalam dua bentuk, yakni perangkat terdedikasi atau sebagai perangkat lunak yang diinstalasikan dalam sebuah *server. Network firewall* secara umum memiliki beberapa fitur utama, yakni apa yang dimiliki oleh *personal firewall* (*packet filter firewall* dan *stateful firewall*), *Circuit Level Gateway*, *Application Level Gateway*, dan juga NAT *Firewall*. *Network firewall* umumnya bersifat transparan (tidak terlihat) dari pengguna dan menggunakan teknologi *routing* untuk menentukan paket mana yang diizinkan, dan mana paket yang akan ditolak.

3. PERANCANGAN DAN IMPLEMENTASI

3.1. Akses *policy* dan *log* pada Fortigate

Pada rancang bangun ini *firewall* yang digunakan adalah Fortigate yang ditempatkan pada garis terdepan yang memisahkan antara wilayah internet dan intranet, sehingga dibutuhkan sistem keamanan dan *log* yang handal sebagai tindakan pencegahan terhadap ancaman dan serangan dari dalam maupun luar sistem jaringan komputer. Adapun *policy* konfigurasi sistem jaringan yang digunakan adalah :



Gambar 1. Desain akses *policy*

Pencatatan *log* lalu lintas data jaringan komputer yang akan dilakukan pada *firewall* adalah :

1. Anti virus
   - *Virus Scan* (HTTP, FTP dan SMTP)
   - *File Filter* (HTTP, FTP dan SMTP)
2. *Web Filtering*
   - *Web Content Filter*
   - *Web URL Filter*
   - FortiGuard *Web Filtering*
3. Kontrol aplikasi
   - *Instant Messaging*
   - *Anonymous Proxy*
   - *Peer-to-peer*
   - *Botnet*
   - *VoIP*

Pencatatan *log* lalu lintas data jaringan komputer tersebut berlaku bagi semua akses masuk maupun keluar yang melalui *firewall* dengan kondisi *block* dan *allow.*

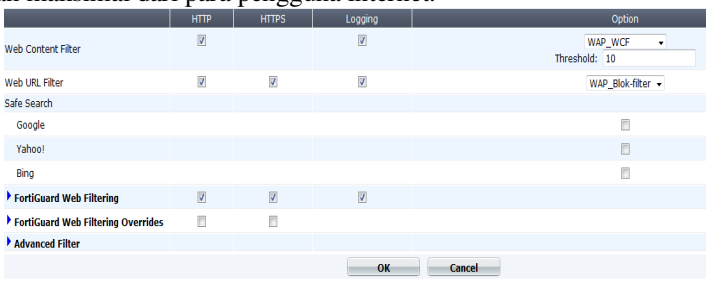
3.1.1 Anti virus

Anti virus pada *firewall* Fortigate berfungsi melakukan pemindaian lalu lintas akses data pada jaringan komputer yang mencakup berbagai modul dan sistem yang bekerja secara terpisah, beberapa model proses yang dilakukan *firewall* berdasarkan berikut ini :

1. Fungsionalitas Antivirus
   - *File size*
   - *File pattern*
   - *File type*
   - *Virus scan*
   - *Grayware*
   - *Heuristics*
2. *File filter*
   - *File pattern*
   - *File type*

3.1.2 Web Filtering

Tiga (3) fungsi utama dari *web filtering* pada *firewall* adalah *Web Content Filter, Web URL Filter*, sistem ini dinamakan *FortiGuard Web Filtering* yang saling berinteraksi satu sama lain untuk memberikan kontrol dan perlindungan maksimal dari para pengguna internet.

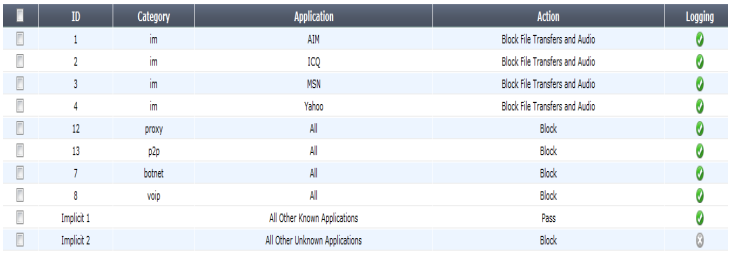


Gambar 2. Tampilan *web filtering*

3.1.3 Kontrol aplikasi

Kontrol aplikasi pada *firewall* merupakan fitur yang berfungsi sebagai pendeteksi dan pengambil tindakan terhadap lalu lintas data jaringan komputer, tergantung aplikasi yang berjalan pada jaringan tersebut. Selain itu aplikasi kontrol ini juga dilengkapi dengan protokol *decoder* perlindungan dari penyusupan sehingga lebih mudah dan handal dalam pengelolaan aplikasi-aplikasi yang melewati jaringan komputer.

Pada penelitian ini hanya beberapa kontrol aplikasi yang akan dipantau berdasarkan tingkat keamanan dan kegunaannya saja.



ID	Category	Application	Action	Logging
1	im	AIM	Block File Transfers and Audio	
2	im	ICQ	Block File Transfers and Audio	
3	im	MSN	Block File Transfers and Audio	
4	im	Yahoo	Block File Transfers and Audio	
12	proxy	All	Block	
13	p2p	All	Block	
7	botnet	All	Block	
8	voip	All	Block	
Implicit 1		All Other Known Applications	Pass	
Implicit 2		All Other Unknown Applications	Block	

Gambar 3. Tampilan kontrol aplikasi

3.2. Pengujian Sistem Pencegahan Penyusupan Pada Jaringan Komputer Berbasis Cyberoam

3.2.1. Instalasi dan koneksi Cyberoam iView

Setelah perencanaan dan implementasi pada *firewall* Fortigate selesai dilakukan, langkah selanjutnya adalah instalasi aplikasi Cyberoam iView sebagai *log analyzer* lalu lintas data yang terjadi pada jaringan komputer, adapaun spesifikasi perangkat minimal yang dibutuhkan adalah :

a. Prosesor Pentium IV with 2GHz
b. RAM 2GB (minimum)
c. Hard Disk Drive SATA/SCSI 30GB (minimum)
d. Sistem Operasi Windows/ Linux

Cyberoam iView selain dapat digunakan untuk analisa lalu lintas data pada jaringan komputer yang menggunakan *firewall* Fortigate juga pembuatan pelaporan akses. Cyberoam iView merupakan aplikasi berbasis *open source* SIEM yang dapat berjalan pada sistem operasi Windows dan Linux, selain itu juga dapat berintegrasi dengan berbagai perangkat jaringan seperti :

1. Linux IPtables / Netfilter Firewall
2. Cyberoam
3. Fortigate
4. Sonicwall
5. Squid
6. Produk-produk yang mendukung *Syslog*.

Untuk menghubungkan aplikasi Cyberoam iView yang telah terinstall dengan *firewall* Fortigate, perlu ditambahkan *setting* pada *firewall* Fortigate yaitu *log setting* → *Remote Logging & Archiving* → *Syslog* dengan mendefinisikan IP/ FQDN server Cyberoam iView.

3.2.2. Hasil pemantauan berbasis Cyberoam iView

Berikut adalah hasil utama pemantauan *log event* lalu lintas data pada jaringan komputer yang ditangkap berdasarkan rancang bangun diatas :

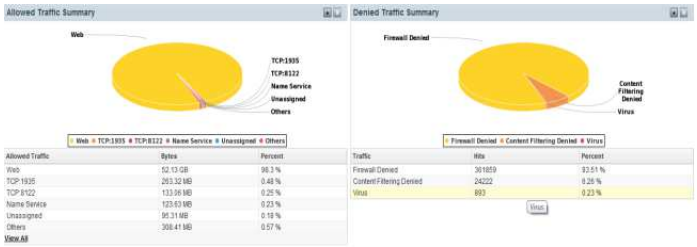
a. *Virus log*

Pemantauan *log* ini memberikan laporan komprehensif untuk melakukan analisa penyusupan dengan dukungan berbentuk grafik tentang lalu lintas virus yang ada pada jaringan komputer.

Gambar 4. Hasil pemantauan lalu lintas virus

b. *Allowed & denied traffic*

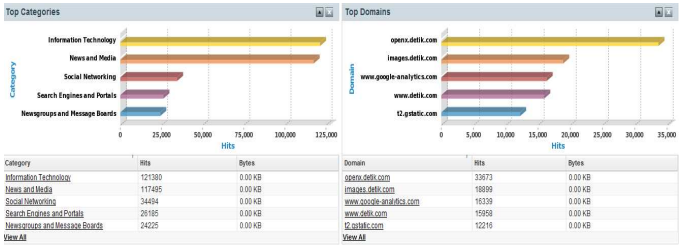
Pemantauan ini berfungsi memberikan laporan yang komprehensif dan grafis tentang lalu lintas data, penggunaan *bandwidth* serta aplikasi dan *host* yang paling banyak digunakan pada jaringan komputer sehingga mempermudah melakukan analisa akses.



Gambar 5. Hasil pemantauan lalu lintas jaringan

c. *Web usage*

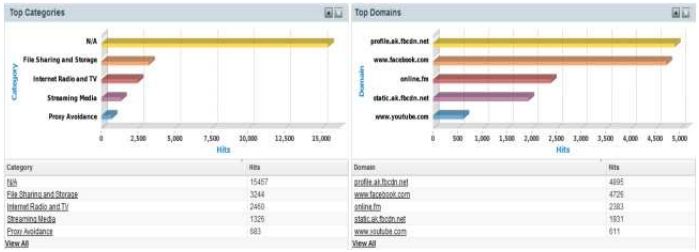
Berfungsi untuk memantau lalu lintas pada jaringan komputer sesuai dengan *policy* aplikasi yang berjalan berdasarkan kategori, domain, isi, tujuan dan aplikasi, sehingga analisa penyusupan pada jaringan komputer lebih mudah.



Gambar 6. Hasil pemantauan *web usage*

d. *Blocked web attempts*

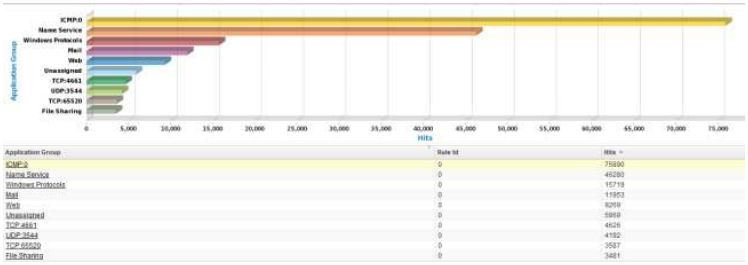
Berfungsi untuk memantau lalu lintas jaringan komputer sesuai dengan *policy* yang tidak diperbolehkan berdasarkan kategori, domain, isi, tujuan dan aplikasi, sehingga analisa penyusupan pada jaringan komputer lebih mudah.



Gambar 7. Hasil pemantauan *blocked web attempts*

e. Kontrol Aplikasi

Merupakan pendekatan komprehensif untuk memahami pola aktifitas secara historis untuk mengidentifikasi aplikasi yang berasal dari dalam maupun luar sistem jaringan.



Gambar 10. Hasil pemantauan kontrol aplikasi

Selain sistem pelaporan yang berbentuk grafik, hasil *log capture* diatas dapat disimpan dalam bentuk Microsoft Excel maupun PDF sebagai data pendukung analisa yang terdokumentasi bahkan sebagai bahan *digital forensic*.

4. KESIMPULAN

Rancang bangun sistem pencegahan penyusupan pada jaringan komputer berbasis Cyberoam telah selesai diujicoba dan berupaya sesuai dengan rancangan sistem jaringan komputer yang diinginkan, sehingga dapat diambil kesimpulan bahwa :

1. Cyberoam dapat diintegrasikan dengan *proprietary firewall* sebagai perangkat yang handal untuk pencegahan dan penganggulangan terjadinya penyusupan ke dalam jaringan komputer;
2. Cyberoam dapat menjadi solusi yang efektif dan efisien sebagai sistem peringatan dini pada lalu lintas jaringan komputer dengan lengkapnya dukungan grafik dan pelaporan sebagai bahan analisa;
3. Mencegah serangan-serangan dari dalam atau luar dengan menggunakan fitur pelaporan yang ada pada Cyberoam.

PUSTAKA

Cyberoam iView product overview, Diakses pada 17 Februari 2011 dari http://www.cyberoam-iview.org/productoverview.html.

Dr. Thomas W. Shinder, Cherie Amon, Robert J. Shimonski, Debra Littlejohn Shinder, 2003, *The Best Damn Firewall Book Period,* Syngress Publishing, Inc.

Elitecore, 2009, *Cyberoam iView linux installation guide.*

Firewall, Diakses pada 17 Februari 2011 dari http://id.wikipedia.org/wiki/Firewall.

Fortinet, 2009, *Fortigate administration guide version 4.0.*

Fortigate® *appliances.* Diakses pada 17 Februari 2011 dari http://www.fortinet.com/products/ fortigate/.

Security Information and Event Management, Diakses pada 17 Februari 2011 dari http://en.wikipedia.org/wiki/SIEM.

Unified Threat Management (UTM), Diakses pada 17 Februari 2011 dari http://deris.unsri.ac.id/ materi/security/UTM.pdf.