FCAPS - *Security Management*

Aria Nasbi

Sistem Komputer, Universitas Sriwijaya, Jl. Raya Palembang-Prabumulih Km.32
Indralaya Ogan Ilir Sumatera Selatan, 30662

Email:nasbiaria17@gmail.com

Abstrak – Manajemen jaringan adalah suatu usaha untuk memelihara seluruh sumber jaringan dalam keadaan baik. Karena saat ini jaringan sangat kompleks, dinamika dan terdiri atas komponen yang tidak dapat diandalkan, peralatan yang baik diperlukan untuk mengelola jaringan tersebut. *Network Management Security* (NMS) yang didesain untuk *monitoring*, memelihara, dan mengoptimalkan jaringan. NMS juga dapat digunakan untuk memonitor komponen *hardware* maupun *software* dalam suatu jaringan dengan tujuan memudahkan pekerjaan *administrator*. Adapun peran *network engineer* menggunakan *network management system* untuk menangani beragam operasi. Salah satu perangkat lunak atau *software* yang digunakan dalam NMS adalah FCAPS. FCAPS yang merupakan model dan *framework* dari *International Organization for Standardization* (ISO) *Telecommunications* yang akan mengkategorikan tujuan kerja dari manajemen jaringan yang terbagi menjadi lima tingkatan yaitu *Fault, Configuration, Accounting, Performance, Security.*

Kata kunci – *Network Management System (NMS), FCAPS, Security Management*

1. Pendahuluan

Perkembangan teknologi informasi saat ini semakin cepat, khususnya teknologi keamanan jaringan yang menjadi salah satu teknologi yang harus diperhatikan ketika suatu sistem atau teknologi terkoneksi dengan jaringan. Maraknya kasus serangan pada jaringan komputer terjadi karena tanpa disadari bahwa pihak komputer yang diserang tidak mengetahui bahwa telah terjadi serangan di dalam sistemnya. Oleh karena itu khususnya sisi *monitoring* sangatlah penting karena selain untuk melihat segala bentuk *anomaly* dan permasalahan di dalam jaringan, juga sangat diperlukan untuk menganalisa suatu jaringan agar dapat dikembangkan oleh pihak *engineering*[1]. Penerapan *network management* dan *monitoring* telah banyak dimanfaatkan oleh berbagai perusahaan, sistem yang digunakan untuk melakukan manajemen dan monitoring jaringan. *Network monitoring system* merupakan sebuah sub sistem dalam manajemen jaringan yang melibatkan penggunaan perangkat lunak dan perangkat keras.

Pada penelitan sebelumnya *tools* yang digunakan adalah *Security Information And Event Management* (SIEM). SIEM adalah teknologi memberikan keamanan TI yang mengadopsi metodologi yang digunakan untuk menkorelasi *log*, peristiwa, mengalir dari komputasi perangkat, sistem dan layanan terdistribusi dengan *baseline* keamanan[2]. Dan pada saat ini terdapat FCAPS *(Fault, Configuration, Accounting, Performance and Security)* management sebagai alat yang memudahkan bagi administrator jaringan untuk melakukan managemen jaringan.

2. Teori Dasar

2.1 *Pengertian Network Management System* (NMS)

Network Management System (NMS) adalah sebuah aplikasi atau serangkaian aplikasi yang mengijinkan network engineer untuk mengelola komponen independen jaringan di dalam kerangka kerja *(framework)* manajemen jaringan yang lebih besar serta di diatur untuk mengawasi seluruh jaringan dan komponen individual dalam jaringa[3]. NMS mengacu pada

software yang digunakan untuk mengelola jaringan. *Network management system* didesain untuk monitoring, memelihara, dan mengoptimalkan jaringan. NMS juga dapat digunakan untuk memonitor komponen hardware maupun software dalam suatu jaringan. *Network engineer* menggunakan *network management system* untuk menangani beragam operasi seperti: mendeteksi perangkat di jaringan sehingga dapat dikenali dan dapat dikonfigurasi dengan benar, jika terjadi gangguan pada sistem maka NMS akan segera memberikan peringatan secara proaktif kepada *engineer*, memonitor kinerja, dan terakhir adalah menganalisa kinerja karena NMS digunakan untuk melacak indikator data kinerja *(performance data indicators)* termasuk *packet loss, latency, bandwidth utilization*, dan lain-lain.

Network management system (NMS) sangat berguna dalam *network device discovery*, *network device monitoring, network performance analysis, network device management,* pemberitahuan atau peringatan yang dapat disesuaikan.

Menurut[1] Faktor yang mempengaruhi manajemen sistem jaringan ini, yaitu :

a. Mengendalikan assets strategi perusahaan.

b. Mengendalikan kompleksitas jaringan.

c. Meningkatkan pelayanan dari suatu jaringan.

d. Menyeimbangkan segala keperluan.

e. Mengurangi *downtime* karena tiap elemen dapat termonitor dengan baik.

f. Mengendalikan biaya.

Tabel 2.1 Proses yang terjadi pada aspek manajemen jaringan

Aspek Manajemen Jaringan	Penjelasan
Network Installation	Berhubungan dengan pelaksanaan proses *instalasi* pada suatu jaringan, misalnya ketika ada suatu
Network Repair	Berhubungan dengan proses perbaikan atau reparasi pada jaringan
Network Test	Berhubungan dengan proses pengetesan atau uji coba pada jaringan
Network Planning & Design	Proses perencanaan dan perancangan jaringan
Fault Management	Berhubungan dengan pendeteksian, dan proses restorasi service atau komponen yang mengalami error
Configuration Management	Berhubungan dengan proses konfigurasi di dalam jaringan
Security Management	Berhubungan dengan proses penanganan keamanan dalam jaringan, misalnya proses pengalokasian privilege kepada user yang berhak mengakses jaringan
Accounting Management	Berhubungan dengan proses administrasi biaya yang diperlukan dalam pengembangan jaringan dan melakukan pengalokasian biaya
Inventory Management	Berhubungan dengan proses manajemen komponen jaringan yang ada, meliputi penentuan apa yang harus ada di dalam jaringan, dan perawatan komponen jaringan

	yang ada
Data Gathering & Analysis	Berhubungan dengan proses pengumpulan dan penganalisisan data pada jaringan
Traffic Management / Performance Management	Berhubungan dengan optimasi performansi dari suatu jaringan

2.2 Pengertian FCAPS Management

FCAPS *(Fault, Configuration, Accounting, Performance, Security) management* merupakan suatu kerangka kerja manajemen jaringan yang di buat oleh Organisasi Internasional untuk Standardisasi (ISO) dan telah menetapkan model fungsional untuk manajemen jaringan. Menurut model ini, ada lima area fungsional manajemen jaringan yaitu Manajemen Kesalahan, Konfigurasi, Akuntansi, Kinerja dan Keamanan[4]. Adpun pengertian dari 5 model fcaps telah di artikan dalam tabel 2.1 di atas. Adapun tujuan dari monitoring yang sesuai dengan FCAPS adalah dengan untuk mengumpulkan informasi yang berguna dari bagian
jaringan sehingga dapat diatur dan dikontrol dengan menggunakan informasi yang telah dikumpulkan. Adapun manfaat lain dari penggunaan monitoring jaringan, yaitu:

1. Untuk mengawasi kejadian yang sedang terjadi didalam jaringan yang memiliki host banyak tanpaalat pengawasan yang baik.
2. Mengetahui masalah pada jaringan sebelum manager menanyakan kepada administrator dan sebelum pelanggan melakukan komplain.
3. Memberikan laporan masalah pada jaringan kepada administrator secara cepat.
4. Mendokumentasikan jaringan.
5. Menjaga agar jaringan selalu dalam kondisi sehat.

Untuk itu, paper ini hanya akan membahas terkait FCAPS tentang *security management,* pada sebuah perusahaan akan sangat dituntut untuk dapat melakukan pengamanan secara sistematis demi mendukung terlaksananya kegiatan produksi secara baik dan optimal.

3. Pembahasan

3.1 FCAPS - *Security Management*

Keamanan menjadi salah satu teknologi yang perlu diperhatikan ketika suatu sistem yang terkoneksi dengan system jaringan komputer menjadi hal yang sangat krusial[5]. Pada saat ini kebutuhan manusia sangat tergantung dengan adanya informasi ataupun data, khususnya informasi atau data digital. Semakin besar kebutuhan adanya informasi semakin meningkat pula insiden atau gangguan keamanan terhadap system jaringan yang meningkat tajam. Hal ini umumnya terjadi dikarenakan masih kurangnya kepedulian terhadap keamanan sebuah sistem khususnya pada infrastruktur hardware jaringan komputer yang masih sangat kurang.

Manajemen keamanan melakukan pendekatan keamanan yang paling umum digunakan terdiri dari pemantauan jaringan untuk pola ancaman yang dikenal[6]. Untuk meningkatkan keamanan dibutuhkannya perangkat-perangkat keamanan yang kuat serta untuk saat ini peran *machine learning* yang bertujuan penyelidikan secara luas dan mendeteksi pola-pola serangan yang kompleks dari data historis yang akan menghasilkan aturan umum untuk memungkinkan mendeteksi variasi serangan yang diketahui.

Pada penelitian[7] "Keamanan" berarti fakta untuk menyelesaikan tugas manajemen keamanan dalam jaringan maka dengan menggunakan perkiraan dibawah ini:

$$S_f \in \{< no >,< partially >,< all >\} = \{0,1,2\}$$
with the criterion $S_f \rightarrow \max$. **…(1)**

Tujuan utama dari *security management* adalah untuk mengatur akses terhadap sumber jaringan sesuai dengan aturan yang telah disetujui, sehingga jaringan tidak bisa diserobot secara sengaja ataupun tidak sengaja. Sebuah subsistem manajemen *security*, misalnya, dapat memonitor semua user yang masuk ke dalam jaringan, dan menolak user yang tidak memiliki kode akses yang benar.

Langkah pertama dari keamanan jaringan adalah aturan dan prosedur yang jelas. Langkah selanjutnya adalah masalah teknis. Protokol utama di dalam *security management* adalah TACACS *(Terminal Access Controller Access Control System),* protokol standard yang digunakan untuk melakukan fungsi-fungsi AAA *(Authentication, Authorization, and Accounting).*

1. Authentication

Authentication adalah proses mengidentifikasi user sebelum user diperbolehkan masuk ke dalam suatu router atau switches.

2. Authorization

Authorization memberikan pengaturan remote access. Di dalam sebuah router Cisco, tingkat authorization bervariasi dari 0 sampai 15, di mana 0 paling rendah dan 15 paling tinggi.

3. Accounting

Accounting digunakan untuk mengumpulkan dan mengirimkan informasi keamanan dan bisa dipergunakan untuk *billing, auditing and reporting*. Informasi yang dikumpulkan adalah identitas *user, start and stop times* dan perintah apa yang dijalankan. *Accounting* memungkinkan *network manager* untuk melacak layanan apa saja yang diambil user beserta berapa banyak sumber jaringan yang diserap.

4. Kesimpulan

FCAPS merupakan suatu kerangka kerja jaringan dengan lima model yang telah di tetapkan oleh *International Organization for Standardization* (ISO) yang akan digunakan dalam *network management system* yang bertujuan untuk melakukan *monitoring* terhadap lalu lintas jaringan. Adapun *security management* yang terdapat dalam FCAPS adalah suatu kewajiban untuk diperhatikan ketika suatu sistem yang terkoneksi dengan system jaringan komputer. Tujuan utama dari *security management* adalah untuk mengatur akses terhadap sumber jaringan sesuai dengan aturan yang telah disetujui, sehingga jaringan tidak bisa diserobot secara sengaja ataupun tidak sengaja dengan dan dengan melakukan fungsi-fungsi dari AAA *(Authentication, Authorization, and Accounting).*

Referensi

[1] P. W. Purnawan and U. B. Luhur, “Managed Service Network Management System(Nms) Berdasarkan Fault , Configuration , Accounting , Performance , Security (Fcaps) Management Managed Service Network Management System (Nms) Berdasarkan Fault , Configuration , Accounting , Performance ,” no. January, 2018.

[2] A. Pratama, A. Wijaya, and R. N. H. D, “Penerapan Network Monitoring Menggunakan Security Information and Event Management (Siem) Berbasis Open Source Di Universitas Bina Darma Palembang,” *Mhs. Tek. Inform. Univ. Bina Darma*, pp. 1–8, 2016.

[3] T.-S. Chou and N. Hempenius, “An Assessment of Practical Hands-On Lab Activities in Network Security Management,” *J. Cybersecurity Educ. Res. Pract.*, vol. 2019, no. 2, p. 2, 2020.

[4] M. Solehfuddin, Sugiyono, and M. Awaludin, “Penerapan Simple Network Management Protocol Pada Fcaps Untuk Monitoring Server Berbasis Android Studi Kasus Pt Jaring Synergi Mandiri,” *CKI SPOT*, vol. 9, no. 2, pp. 119–126, 2016.

[5] S. Khadafi, B. Meilani, and S. Arifin, “SISTEM KEAMANAN OPEN CLOUD COMPUTING MENGGUNAKAN MENGGUNAKAN IDS (INTRUSION DETECTION SYSTEM) DAN IPS (INTRUSION PREVENTION SYSTEM),” *J. IPTEK*, vol. 21, p. 67, Dec. 2017.

[6] S. Ayoubi *et al.*, “Machine Learning for Cognitive Network Management,” *IEEE Communications Magazine*, no. January, pp. 158–165, 2018.

[7] M. Al Rawajbeh, V. Sayenko, and M. I. Muhairat, “Simplified CBA concept and express choice method for integrated network management system,” *Int. J. Comput. Networks Commun.*, vol. 8, no. 3, pp. 47–65, 2016.