IMPLEMENTASI FCAPS DALAM SEGI SECURITY MANAGEMENT PADA PERANGKAT FIREWALL FORTIGATE 1000D

Ryan Darmawan Siregar
Jurusan Sistem Komputer, Universitas Sriwijaya Palembang
Jl. Srijaya Negara, Bukit Besar, Kec. Ilir Bar. I, Kota Palembang, Sumatera Selatan 30128, Indonesia
E-mail: ryandarmawan@outlook.com

Abstrak

Penggunaan firewall pada suatu jaringan perkantoran merupakan suatu tujuan dalam mengamankan komunikasi di dalam suatu jaringan. Hal tersebut berguna dalam mengamankan asset perusahaan seperti server, pengguna, dan perangkat keras yang terhubung langsung ke jaringan. Pada studi kasus ini, implementasi manajemen FCAPS pada segi *security management* merupakan studi kasus dimana manajemen ini dapat meninjau akan manajemen keamanan yang ada pada perusahaan terhadap *firewall* yang digunakan. Penerapan security management ini sendiri diharapkan dapat memetakan sekaligus mengetahui akan tingkat keamanan terhadap suatu jaringan yang dikelola oleh administrator.

Kata kunci: FCAPS, security management, Firewall

Abstract

The use of a firewall on an office network is an objective in securing communication on a network. This is useful in securing company assets such as servers, users and hardware that are connected directly to the network. In this case study, the implementation of FCAPS management in terms of security management is a case study where this management can review the company's existing security management of the firewall used. The application of security management itself is expected to be able to map at the same time knowing the level of security of a network managed by an administrator.

Keywords: FCAPS, security management, Firewall

1. Pendahuluan

Pada perkembangan teknologi di beberapa dekade ini, perkembangan pesat sebuah teknologi tak luput dari inovasi dan riset yang berlangsung. Pada perkembangannya, tentu ada sisi positif seperti mudahnya melakukan komunikasi hingga pertukaran data dan sisi negatifnya yaitu serangan dan pencurian data. Pencurian data dan serangan sering kali menjadi sorotan publik akan kuatnya perkembangan teknologi dimana semakin mau teknlogi maka serangan dan pencurian menjadi semakin tinggi dengan model yang canggih. Hal ini dibutuhkan sebuah keamaan untuk memproteksi suatu jaringan. Dalam penanganan dan implementasi, keamanan tersebut perlu diatur dan dimonitoring didalam sebuah standar agar pergerakannya teratur.

Dalam pergerakannya, suatu jaringan dapat melakukan monitoring ke beberapa sektor manajemen, hal ini meliputi *Fault Management, Configuration Management, Accounting Management, Performance Management, dan Security Management*. Hal tersebut biasa dikenal dengan FCAPS manajemen. Manajemen ini nantinya berguna baik untuk *Network Management System* (NMS) hingga administrator dan tim IT yang menjaga semua aspek dari infrastruktur jaringan[1].

Pada permasalahan yang diangkat pada paper, penulis melakukan implementasi terhadap manajemen FCAPS di segi *security management*. Hal ini dilakukan guna melihat kemampuan akan suatu firewall dalam menjalankan keamanan sesuai manajemen yang dipilih.

2. Tinjauan Pustaka

2.1 FCAPS

FCAPS merupakan nama berdasarkan standarisasi internasional (ISO) terhadap TMN Model dan Framework pada network management yang memiliki singkatan dari *Fault Management,*

Configuration Management, Accounting Management, Performance Management, dan *Security Management* dalam sebuah jaringan. FCAPS merupakan manajemen jaringan yang memiliki kemampuan dalam mengontrol dan melakukan monitor jaringan komputer[2][3].

2.1.1. Security Management

Merupakan fungsi yang digunakan untuk mengatur akses baik ke sumber daya jaringan sehingga tidak memungkinkan terjadi kebocoran informasi dikarenakan informasi yang diperoleh harus berizin. Hal ini dapat dilakukan dengan melakukan beberapa cara seperti pembatasan akses pengguna ke dalam sumber daya jaringan, memberi pemberitahuan terhadap administrator jaringan mengenai penyusupan ataupun usaha-usaha pelanggaran keamanan yang membahayakan sumber daya jaringan. Security Management merupakan bagian dari fungsi standar ITU-T M.3010[4].

Berdasarkan fitur-fitur yang berkolerasi dengan fungsi-fungsi *security management* adalah sebagai berikut:

a) Security Related Information Distribution
Industry-leading protection: *NSS Labs Recommended*, *VB100*, *AV Comporatives*, dan *ICSA validated security and performance*. Pada perangkat FortiGate 1000D, hal ini merupakan bagian sertifikasi dimana perangkat FortiGate 1000D memiliki segala sertifikasi yang dimaksud.

b) *Security Audit Trial Log*
Melakukan kontrol di ribuan aplikasi, melakukan pemblokiran terhadap eksploitasi terbaru, melakukan filter di lalu lintas web berdasarkan jutaan peringkat *real-time* URL. Pada perangkat FortiGate 1000D, fitur tersebut ada pada *Web Filter, Application Control, Virtual Intrusion Prevention System*.

c) Access Log
Melakukan identifikasi dan kontrol akses jaringan untuk berbagai jenis perangkat yang ada di dalam jaringan.Pada perangkat FortiGate 1000D, fitur tersebut ada pada *physical topology*.

2.2 *Firewall*

Firewall merupakan suatu sistem atau perangkat yang memberi otorisasi pada lalu lintas jaringan komputer yang dianggap aman atau memenuhi syarat untuk melaluinya dan melakukan monitoring maupun pencegahan pada lalu lintas jaringan komputer yang dianggap tidak aman ataupun tidak memenuhi syarat[5].

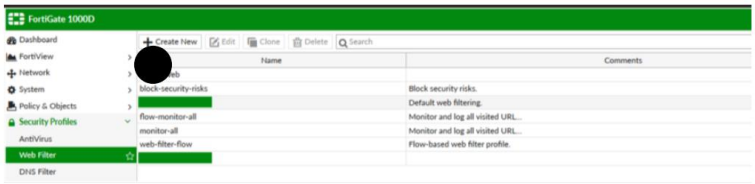
3. Hasil dan Analisa

3.1 Kofigurasi FortiGate 1000D Sesuai dengan Korelasi Security Management

Pada konfigurasi *firewall* FortiGate 1000D pada aspek *security management*, terdapat beberapa fitur yang sudah diaktifkan oleh administrator, baik pengaktifan sesuai dengan masukkan administrator maupun sesuai standar pabrik. Penjelasan fitur-fitur tersebut adalah sebagai berikut:

3.1.1. *Web Filter*

Fitur *web filter* digunakan untuk menyaring baik membatasi maupun melakukan pemblokiran terhadap situs web yang tidak diperbolehkan untuk diakses. Fitur ini biasanya memiliki daftar-daftar situs yang tidak diperbolehkan untuk diakses karena alasan keamanan. Tampilan *Web Filter* terdapat pada gambar 3.1.



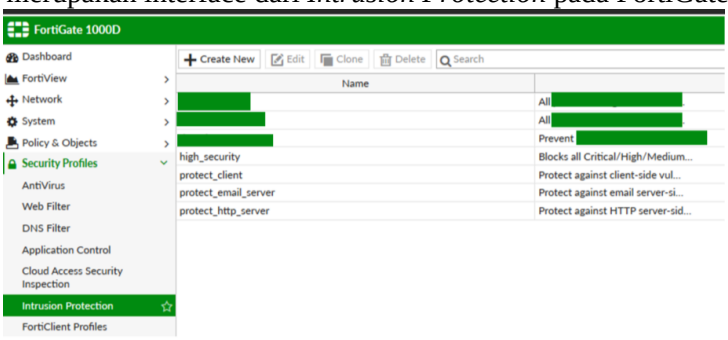
Gambar 3.1

Adapun jenis-jenis aksi yang terdapat pada Web Filter yaitu *Allow, Block, Warning, Authenicate,* dan *Monitor.*

Pada fungsi dan aksi yang ada pada *web filter*, hal ini berguna untuk mengurangi terjadinya pembobolan diakibatkan oleh *malware* akibat akses sembarang web yang berbahaya. Hal tersebut guna menghindari kerusakan baik perangkat komponen klien maupun perangkat infrastruktur jaringan.

3.1.2. *Intrusion Protection*

Fitur *Intrusion Protection* merupakan fitur dalam FortiOS yang menggerakan *Intrusion Prevention System. Intrusion Prevention System* (IPS) adalah teknologi yang difungsikan untuk melindungi jaringan dari serangan penjahat siber. Teknologi IPS bekerja dengan melakukan *seeking* dan *blocking* ancaman dari luar secara aktif. Maka, dengan teknologi IPS dapat menghindari ancaman sebelum mencapai perangkat yang rentan berpotensi terkena serangan. Pada gambar 3.2 merupakan interface dari *Intrusion Protection* pada FortiGate 1000D.



Gambar 3.2

Teknologi IPS memiliki dua Teknik untuk mencegah serangan dari luar yaitu dengan menggunakan *anomaly-based defense* dan *signature-based defense*. Penjelasan keduanya sebagai berikut:

a) Teknik *anomaly-based defense*

Digunakan ketika lalu-lintas jaringan digunakan sebagai senjata. Hal ini dapat menyebabkan *host* dapat dibanjiri dengan lalu lintas yang jauh lebih banyak tetapi hanya sedikit yang dapat diselesaikan. Contohnya seperti serangan *Denial of Service* (DoS). Dalam menghindari DoS, dapat digunakan *Access Control Lists* (ACL) untuk mengatur rentang IP/*Subnet*/*Ranges* pada DoS *policy.*

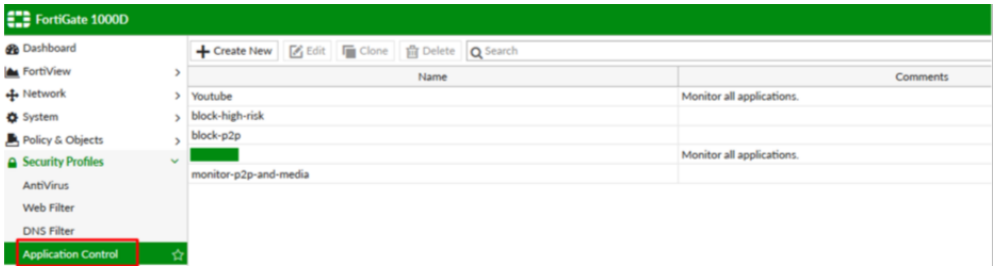
b) Teknik *signature-based defense*

Digunakan ketika serangan tersebut diketahui ataupun dieksploitasi letak kerentanannya. Serangan ini sering melibatkan *attacker* untuk mendapatkan akses ke jaringan. Untuk mendapatkan akses, *attacker* berupaya untuk berkomunikasi dengan *host*. Komunikasi ini mencakup perintah ataupun urutan perintah dan juga beberapa variabel.

Dalam pergerakannya, IPS bererja berdasarkan IPS *Sensor*. IPS *Sensor* ini berisi database tentang ciri-ciri serangan, sehingga ketika terdapat kecocokan *pattern* maka firewall dapat langsung mengeksekusi-nya.

3.1.3. *Application Control*

Fitur *Application Control* digunakan untuk melakukan pemeriksaan lalu lintas jaringan yang dibuat oleh aplikasi yang ingin di kontrol. Terdapat beberapa kategori pengontrolan seperti *allow* yang digunakan untuk memperbolehkan aplikasi lewat, *monitor* yang digunakan untuk melakukan pengawasan sekaligus melihat jejak dari aplikasi tersebut, *block* digunakan untuk menutup akses ke aplikasi tersebut, *quarantine* digunakan untuk meng-karantina terhadap akses aplikasi, dan *view signature* yang digunakan untuk selalu melihatkan tanda keamanan yang berupa sertifikat keamanan dari aplikasi tersebut.



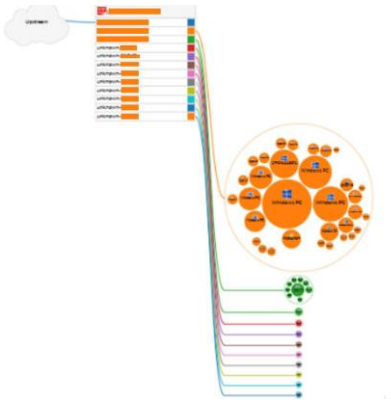
Gambar 3.3

3.1.4. *Physical Topology*

Fitur *physical topology* merupakan fitur dimana menampilkan jumlah perangkat yang terhubung ke jaringan. Fitur ini menampilkan jumlah perangkat kedalam bentuk gelembung, dan juga menggambarkan penggunaan bandwidth di dalam jaringan. Penggunaan konsol ini dapat mem-filter berdasarkan *traffic* perangkat, hitungan perangkat, jenis perangkat, atau tidak ada perangkat.

Penggunaan konsol *physical topology* dapat membantu administrator untuk melihat perangkat yang terhubung di jaringan hingga mengetahui informasi siapa saja yang terhubung. Konsol ini juga dapat melacak keberadaan *user* yang terhubung di jaringan.

Pada gambar 3.4 terlihat bagaimana keadaan *physical topology* tersebut. Penulis melihat bahwasannya bentuk *physical topology* dapat berubah-ubah sesuai keadaan waktu. Sebagai contoh, jumlah perangkat pada waktu 24 jam yang lalu berbeda dengan jumlah perangkat pada 1 jam yang lalu.



Gambar 3.4

4. Kesimpulan

Kesimpulan, pada manajemen FCAPS di segi *security management* dapat dijadikan oleh suatu perusahaan sebagai acuan baik dalam menilai kinerja jaringan dari perusahaan maupun pencegahan serangan dan mencari titik masalah dalam perbaikan jaringan.

Penggunaan *Security Management* sebagai acuan keamanan, tentu dapat menghindari turunnya nilai SLA dikarenakan dapat menghindari terjadinya *crash* (*fault*) yang disebabkan oleh serangan, sehingga resiko terjadi *downtime* akibat serangan dapat dihindari.

5. Daftar Pustaka

[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, doi: 10.13140/RG.2.2.18486.60481.

[2] D. Mega Paramita and A. Nurul Fajar, “Biomass-Based Analysis of Network Performance Management Dashboard,” *International Journal of Mechanical Engineering and Technology (IJMET)*, vol. 10, no. 3, pp. 952–963, 2019, [Online]. Available:

http://www.iaeme.com/ijmet/issues.asp?JType=IJMET&VType=10&IType=3http://www.iaeme.com/IJMET/issues.asp?JType=IJMET&VType=10&IType=3.

[3] C. Management, A. Management, P. Management, and P. Management, “PENERAPAN NETWORK MANAGEMENT SYSTEM DENGAN WIRESHARK ABSTRACT : Network Management System (NMS) is a function to supervise the performance of the network and taking action to control , monitor traffic flow so that the operating capacity on a network can,” pp. 21–26.

[4] H. Yoo and S. Kim, “Game operation query language for facilitating game server ’ s FCAPS operation,” vol. 17, 2018.

[5] S. J. Fu, H. W. Hsu, Y. C. Kao, S. C. Tsai, and C. C. Tseng, “An autoblocking mechanism for firewall service,” *2017 IEEE Conference on Dependable and Secure Computing*, vol. 3, pp. 531–532, 2017, doi: 10.1109/DESEC.2017.8073877.