

Nama : Muhamad Yusup
NIM : 09011281419061

Analisa Manajemen FCAPS pada Sistem Keamanan Jaringan Menggunakan Firewall FortiGate 1000D

I. Definisi Manajemen Jaringan

Jaringan komputer adalah himpunan "interkoneksi" antara dua komputer atau lebih yang terhubung dengan media transmisi kabel atau tanpa kabel (wireless). Manajemen jaringan merupakan kemampuan untuk mengontrol dan memonitor sebuah jaringan komputer dari sebuah lokasi. The International Organization for Standardization (ISO) mendefinisikan sebuah model konseptual untuk menjelaskan fungsi manajemen jaringan.

Model manajemen jaringan OSI mengkategorikan lima bagian fungsi, yang dikenal sebagai model FCAPS :

1. *Fault Management* (Manajemen Kesalahan / Gangguan), menyediakan fasilitas yang memungkinkan administrator jaringan untuk mengetahui kesalahan (fault) pada perangkat yang dikelola, jaringan, dan operasi jaringan, agar dapat segera menentukan apa penyebabnya dan dapat segera mengambil tindakan perbaikan. Manajemen kesalahan memiliki mekanisme untuk : melaporkan terjadinya kesalahan; mencatat laporan kesalahan; melakukan diagnosis; mengoreksi kesalahan (dimungkinkan secara otomatis).
2. *Configuration Management* (Manajemen Konfigurasi), memonitor informasi konfigurasi jaringan sehingga dampak dari perangkat keras atau pun lunak tertentu dapat dikelola dengan baik. Hal tersebut dapat dilakukan dengan kemampuan inisialisasi, konfigurasi ulang, pengoperasian, dan mematikan perangkat yang dikelola.
3. *Accounting Management* (Manajemen Akuntansi / Pelaporan), mengukur utilisasi jaringan dari pengguna atau grup tertentu untuk : menghasilkan informasi tagihan (billing); mengatur pengguna atau grup, membantu dalam menjaga performa jaringan pada level tertentu yang dapat diterima.
4. *Performance Management* (Manajemen Performa), mengukur berbagai aspek dari performa jaringan termasuk pengumpulan dan analisis dari data statistik sistem sehingga dapat dikelola dan dipertahankan pada level tertentu yang dapat diterima. Untuk itu, manajemen performa memiliki kemampuan untuk : memperoleh utilisasi dan tingkat kesalahan dari perangkat jaringan; mempertahankan performa pada level tertentu dengan memastikan perangkat memiliki kapasitas yang mencukupi.
5. *Security Management* (Manajemen Keamanan), mengatur akses ke sumber daya jaringan sehingga informasi tidak dapat diperoleh tanpa izin. Hal tersebut dilakukan dengan cara : membatasi akses ke sumber daya jaringan; memberi pemberitahuan akan adanya usaha pelanggaran dan pelanggaran keamanan.

II. Firewall FortiGate 1000D

Firewall adalah sistem keamanan jaringan komputer yang digunakan untuk melindungi komputer atau jaringan dari berbagai jenis serangan malware. Dalam definisi lain juga dikatakan bahwa 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 jaringan komputer yang dianggap tidak aman. Firewall dapat berupa perangkat lunak (program komputer atau aplikasi) atau perangkat keras (peralatan khusus untuk menjalankan program firewall) yang berjalan pada pintu gerbang (gateway) antara jaringan lokal dan jaringan lainnya.

Firewall umumnya juga digunakan untuk mengontrol akses terhadap siapa saja yang memiliki akses terhadap jaringan pribadi dari pihak luar. Saat ini, istilah firewall menjadi istilah umum yang merujuk pada sistem yang mengatur komunikasi antar dua jaringan yang berbeda. Mengingat saat ini banyak perusahaan yang memiliki akses internet dan juga jaringan lokal di dalamnya, maka perlindungan terhadap asset digital dan data perusahaan menjadi sangat penting. Jadi dapat disimpulkan bahwa firewall merupakan sebuah mekanisme sistem yang akan melakukan pengawasan dan penyaringan paket yang keluar dan masuk dari jaringan lokal maupun jaringan luar. Paket yang dianggap aman oleh sistem firewall akan diizinkan untuk melewati jaringan, sedangkan paket yang dicurigai akan merusak dan mengganggu sistem jaringan serta end user di dalamnya akan di cegah dan tidak diperbolehkan untuk melalui jaringan.

Fortigate adalah sebuah sistem keamanan yang dikeluarkan oleh perusahaan Fortinet. Fortinet merupakan perusahaan, penyedia layanan, dan badan pemerintah di seluruh dunia, termasuk mayoritas dari perusahaan Fortune Global 100 tahun 2009. Fortinet merupakan pemimpin pasar untuk unified threat management (UTM).

Unified Threat Management atau UTM adalah segmen produk jaringan yang dikhususkan untuk menangani fungsi keamanan jaringan secara terpadu. Pada produk UTM ini menghasilkan Fortigate yang memiliki fitur-fitur seperti firewall, Intrusion Prevention System, web filtering, antivirus yang digabungkan menjadi satu kesatuan dengan tambahan fitur jaringan lain seperti routing dalam satu box hardware.

Fortigate sebagai perangkat yang menjamin keamanan jaringan secara keseluruhan sekaligus berfungsi sebagai gateway dan router bagi jaringan LAN sehingga tak dibutuhkan lagi router ataupun perangkat tambahan load balancing bila ada lebih dari satu koneksi WAN.

Satu perbedaan yang utama, konten FortiASIC yang di custom sendiri serta prosesor jaringan Fortinet memungkinkan sistem Fortigate mendeteksi dan mengeliminir secara real time ancaman yang terintegrasi, bahkan dalam skala kompleks, tanpa menurunkan kinerja jaringan, sementara serangkaian proses manajemen, analisa, database dan solusi perlindungan endpoint bekerja meningkatkan penyebaran fleksibilitas dan memberikan dampak yang nyata dalam mengurangi biaya operasional manajemen keamanan jaringan.

III. Analisa FCAPS

Kelengkapan fungsi manajemen yang dimiliki berdasarkan standard FCAPS. Fitur-fitur di dalam Firewall dikelompokkan ke dalam fungsi manajemen yang terdefinisi dalam standard FCAPS. Berikut fungsi-fungsi manajemen yang terdefinisi pada standard FCAPS :

F	C	A	P	S
Fault detection	Resource initialization	Track service / resource usage	Utilization & error rates	Selective resource access
Fault correction	Network provisioning	Cost for services	Consistent performance level	Enable NE functions
Fault isolation	Auto-discovery	Accounting limit	Performance data collection	Access logs
Network recovery	Backup and restore	Combine costs for multiple resources	Performance report generation	Security alarm / event reporting
Alarm handling	Resource shut down	Set quotas for usage	Performance data analysis	Data privacy
Alarm filtering	Change management	Audits	Problem reporting	User access rights checking
Alarm generation	Pre-provisioning	Fraud reporting	Capacity planning	Take care of security breaches & attempts
Clear correlation	Inventory/asset management	Support for different modes of accounting	Performance data & statistics collection	Security audit trail log
Diagnostic test	Copy configuration		Maintaining & examining historical logs	Security related information distributions
Error logging	Remote configuration			
Error handling	Job initiation, tracking & execution			
Error statistics	Automated software distribution			

Gambar fungsi-fungsi manajemen yang terdefinisi pada standard FCAPS

Terdapat banyak fitur yang ada pada firewall FortiGate 1000D terlepas dari kemampuan utamanya untuk melakukan manajemen keamanan jaringan, seperti menyimpan log yang akan berguna dalam proses auditing dan accounting, alarm terhadap pola perilaku abnormal dalam proses manajemen kesalahan, serta monitoring terhadap performa seluruh asset network dari adanya gangguan keamanan jaringan. Berikut beberapa fitur utama yang ada pada firewall FortiGate yang akan menunjukkan fungsi-fungsi manajemen jaringan yang dikategorikan oleh OSI dalam membantu seorang administrator mendapatkan fungsi optimal dari jaringannya :

No.	Fitur	Fungsi Manajemen yang Berkorelasi	Kategori FCAPS
1	Memiliki sebuah platform yang benar-benar terhubung dengan satu OS untuk semua keamanan dan layanan jaringan untuk semua platform FortiGate	<i>Performance Data & Statistic Collection</i>	<i>Performance Management</i>
2	Industry-leading protection: NSS Labs Recommended, VB100, AV	<i>Security related information distribution</i>	<i>Security Management</i>

	Comparatives, and ICSA validated security and performance.		
3	Mengontrol ribuan aplikasi, memblokir eksploitasi terbaru, dan lalu lintas web filter berdasarkan jutaan peringkat real-time URL	<i>Security audit trial log</i>	<i>Security Management</i>
4	Mencegah, mendeteksi, dan mengurangi serangan canggih secara otomatis dalam hitungan menit dengan perlindungan ancaman canggih yang terintegrasi.	<i>Performance data analysis</i>	<i>Performance Management</i>
5	Memiliki tools konfigurasi FortiExplorer yang memungkinkan administrator untuk dengan cepat konfigurasi akses, termasuk melalui ponsel dan tablet	<i>Remote Configuration</i>	<i>Configuration Management</i>
6	Identifikasi dan kontrol akses jaringan untuk berbagai jenis perangkat hadir pada jaringa	<i>Access Log</i>	<i>Security Management</i>
7	Monitor realtime	<i>Performance Data Collection</i>	<i>Performance Management</i>
8	Memiliki fitur IPS dan integrasi proteksi DoS untuk perlindungan dari pola aktivitas abnormal	<i>Fault Detection, Fault Correction</i>	<i>Fault Management</i>
9	Detil log dan laporan out-of-the-box yang penting untuk kepatuhan, audit, dan tujuan diagnostic	<i>Track Service / Resource Usage</i>	<i>Accounting Management</i>

Secara keseluruhan, analisa dilakukan dengan memperhatikan fitur-fitur utama firewall FortiGate 1000D terhadap fungsi manajemen yang berkorelasi dengan fungsi-fungsi manajemen FCAPS yang telah terdefinisi.

Dalam fungsi *fault management*, firewall FortiGate memiliki fitur untuk mampu mendeteksi pola-pola behavior network yang bersifat abnormal dan memberikan notifikasi kepada administrator melalui email secara langsung sehingga fungsi manajemen kesalahan yang terjadi pada network dapat dimonitoring secara realtime.

Dalam fungsi *configuration management*, firewall FortiGate memberikan fasilitas fungsi pada layanannya untuk melakukan proses remote konfigurasi yang memungkinkan administrator dapat melakukan akses dengan cepat ke network jika dalam kondisi-kondisi tertentu diperlukan.

Dalam fungsi *accounting management*, firewall FortiGate menyediakan sebuah fitur yang mampu memberikan laporan terhadap apa saja yang terjadi pada kondisi keamanan jaringan untuk memenuhi keperluan auditing dan diagnosis jaringan, sehingga administrator mampu untuk melakukan pengelolaan terhadap jaringan yang akan dilakukan selanjutnya berdasarkan proses yang terjadi.

Dalam fungsi *performance management*, terdapat fitur monitoring keadaan network secara real time untuk memberikan gambaran kondisi performa keamanan jaringan yang ada pada network, serta melakukan pengumpulan data terhadap performa network yang ada. Selain itu, keseluruhan layanan dan keamanan pada seluruh perangkat FortiGate akan terintegrasi dalam sebuah platform Forti OS dalam melakukan manajemen performa.

Dan selanjutnya fungsi *security management* di dalam Firewall FortiGate 1000D merupakan letak fitur-fitur utama yang ada pada firewall, seperti kemampuan sistem dalam melakukan distribusi informasi terkait isu-isu keamanan jaringan, mengontrol ribuan aplikasi, memblokir jenis-jenis eksploitasi serta melakukan filtering web berdasarkan database yang dimiliki, serta kemampuannya yang mampu melakukan identifikasi dan kontrol akses jaringan untuk berbagai jenis perangkat hadir pada jaringan.

IV. Kesimpulan

Model manajemen jaringan OSI mengkategorikan lima bagian fungsi, yang dikenal sebagai model FCAPS, diantaranya *Fault Management*, *Configuration Management*, *Accounting Management*, *Performance Management*, dan *Security Management*. Model ini akan membantu akan membantu seorang administrator untuk mendapatkan fungsi optimal dari jaringan. Kelima fungsi ini memiliki keterkaitan satu sama lain, namun dengan porsi yang berbeda-beda. Fungsi keamanan harus menyentuh semua fungsi agar efektif, sedangkan fungsi konfigurasi adalah fungsi yang memegang data penting untuk semua fungsi lainnya.