TUGAS

MANAJEMEN JARINGAN

DI SUSUN OLEH :

MARINI SUPRIANTY

09011181419016

SISTEM KOMPUTER

FAKULTAS ILMU KOMPUTER

UNIVERSITAS SRIWIJAYA

2017

ANALISA *FCAPS* DENGAN LAPORAN KERJA PRAKTIK IMPLEMENTASI CISCO FIREWALL PADA DMZ DI JARINGAN KANTOR PUSAT PT. PUSRI PALEMBANG

FCAPS

Manajemen jaringan mengacu pada pelaksanaan (operation), administrasi (administration), perawatan (maintenance) dan ketentuan yang berlaku (provisioning) pada suatu sistem jaringan.

1. Pelaksanaan (Operation) menjaga agar jaringan dan service-service yang disediakan oleh jaringan tersebut berjalan lancar. Termasuk didalamnya monitoring jaringan untuk mendeteksi masalah secepat mungkin.
2. Administrasi berkaitan dengan pencatatan atau dokumentasi segala sumber daya pada network dan bagaimana sumber daya tersebut digunakan.
3. Perawatan (maintenance) berurusan dengan kegiatan perbaikan, upgrading network, dan menjaga network agar beroperasi maksimal, seperti mengatur konfigurasi parameter perangkat jaringan.
4. Penetapan ketentuan (provisioning) berkaitan dengan melakukan konfigurasi sumber daya network agar dapat memberikan service-service yang diinginkan.

Cara yang umum dalam mengkategorikan fungsi-fungsi dari manajemen network adalah FCAPS – Fault, Configuration, Accounting/Administration, Performance dan Security. FCAPS merupakan model dan framework dari ISO Telecommunications untuk Management Network untuk mengkategorikan tugas tugas dari network management.

1. Fault Management

Tujuan dari Fault Management adalah untuk mengenali, mengisolasi, memperbaiki dan mencatat (membuat log) dari setiap fault yang terjadi pada network. Lebih jauh lagi, jaringan. Fault Management menggunakan analisa untuk memprediksi error yang terjadi agar network selalu beroperasi dengan lancar.

Saat fault terjadi, komponen network mengirim notifikasi kepada network operator menggunakan protocol tertentu seperti SNMP atau paling tidak menuliskan pesan kepada consolenya agar fault ditangkap dan dicatat pada log. Fault log /

catatan-catatan fault merupakan input yang bisa digunakan untuk membangun statistik yang digunakan untuk menentukan service-service apa yang diperlukan bagi setiap network komponen, atau sub network atau bahkan network secara keseluruhan. Statistik tersebut juga dapat digunakan untuk mengetahui komponen network mana yang rapuh/rentan error dan membutuhkan perhatian khusus dari network administrator.

2. Configuration Management

Tujuan dari Configuration Management meliputi :

- Mengumpulkan dan menyimpan konfigurasi dari perangkat-perangkat jaringan.
- Menyederhanakan konfigurasi suatu perangkat.
- Mencatat perubahan yang terjadi pada suatu konfigurasi.
- Melakukan konfigurasi routing.

3. Accounting/Administration Management

Tujuannya adalah untuk mengumpulkan statistic penggunaan setiap user.

Contohnya :

- Penggunaan disk storage
- Penggunaan CPU
- Penggunaan bandwidth

4. Performance Management

Performance management memungkinkan untuk mempersiapkan management di masa yang akan datang(upgrading), dan juga merumuskan efisiensi dari jaringan. Performance Management berkaitan dengan persentase kegunaan perangkat, rasio error dan respons time. Dengan menganalisa data performansi, keadaan jaringan dapat termonitor.

5. Security Management

Security management merupakan proses pengontrolan akses terhadap asset yang ada pada jaringan. Data security bisa diperoleh dengan authentication dan encryption.

	Problem	Solution	Result
Fault	Sistem harus dilindungi dari segala macam serangan dan usaha penyusupan atau pemindaian oleh pihak yang tidak berhak.	Menerapkan DMZ (*Demilitarized Zone)* pada topologi jaringan	Keamanan jaringan lebih terjaga
Configuration	Tidak optimalnya pelayanan jaringan serta ancaman serangan dari pihak luar untuk mensabotase jaringan.	Metode DMZ (*Demilitarized Zone)* menggunakan Cisco Firewall	Mempermudah administrator jaringan untuk menjaga jaringannya agar terhindar dari serangan hacker.
Accounting	Akses konfigurasi yang lebih mudah karena terpisahkan antara DMZ dengan non DMZ	Mengontrol perangkat jaringan sesuai jadwal yang telah ada untuk menjaga stabilitas perangkat.	Efisiensi biaya perawatan perangkat jaringan.
Performance	Monitoring zona non DMZ lebih rumit karena menyatu dengan seluruh topologi	DMZ (*Demilitarized Zone)*	Mengurangi beban kerja administrator untuk mengawasi zona rawan serangan.
Security	Rawan terhadap serangan hacker/pihak lain yang ingin masuk ke system.	Akses DMZ (*Demilitarized Zone)* menggunakan Cisco Firewall	Mencegah bocornya informasi penting yang rentan terhadap ancaman orang luar.

ANALISA

- **F**ault

  Sistem harus dilindungi dari segala macam serangan dan usaha penyusupan atau pemindaian oleh pihak yang tidak berhak. Oleh karena itu, keamanan jaringan komputer sebagai bagian dari sebuah sistem informasi adalah sangat penting untuk menjaga validitas dan integritas data serta menjamin ketersediaan layanan begi penggunanya. Sistem harus dilindungi dari segala macam serangan dan usaha penyusupan atau pemindaian oleh pihak yang tidak berhak. Menerapkan DMZ (*Demilitarized Zone)* pada topologi jaringan membuat keamanan jaringan lebih terjaga.

- **C**onfiguration

Tidak optimalnya pelayanan jaringan serta ancaman serangan dari pihak luar untuk mensabotase jaringan. Maka dari itu digunakanlah Metode DMZ (*Demilitarized Zone)* menggunakan Cisco Firewall. Untuk mempermudah administrator jaringan untuk menjaga jaringannya agar terhindar dari serangan hacker.

- **A**ccounting

  Akses konfigurasi yang lebih mudah karena terpisahkan antara DMZ dengan non DMZ. Mengontrol perangkat jaringan sesuai jadwal yang telah ada untuk menjaga stabilitas perangkat. Efisiensi biaya perawatan perangkat jaringan.

- **P**erformance

  Monitoring zona non DMZ lebih rumit karena menyatu dengan seluruh topologi. Tetapi, DMZ dapat mengurangi beban kerja administrator untuk mengawasi zona rawan serangan.

- **S**ecurity

  Rawan terhadap serangan hacker/pihak lain yang ingin masuk ke system. Karena akses DMZ (*Demilitarized Zone)* menggunakan Cisco Firewall dapat mencegah bocornya informasi penting yang rentan terhadap ancaman orang luar.