Dasar – Dasar Keamanan Jaringan

Modul 2

Muhammad Ogin Hasanuddin

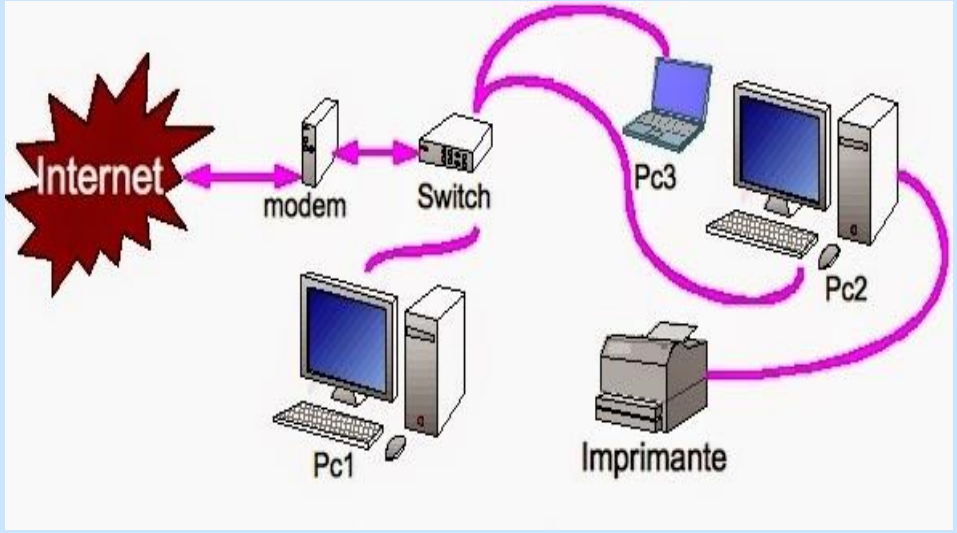
KK Teknik Komputer
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung

- Model Jaringan Client - Server
- Perbedaan Otentifikasi dan Otorisasi
- Berbagai Jenis Firewall di Jaringan Berbeda
- Berbagai Jenis Item Memantau dalam Jaringan
- Cara Memetakan Komponen Jaringan Inti ke Jaringan Komputasi Awan

Model Jaringan Client – Server

Jaringan adalah kumpulan perangkat yang mendukung untuk dapat berkomunikasi dalam kehidupan sehari – hari baik di rumah, tempat kerja, dan area publik. Semua perangkat akan bergantung pada kontrol akses media atau alamat protokol internet (IP) dalam mengirimkan data di jaringan.

1. Network Client, suatu perangkat komputer yang ringan sehingga tidak dapat menjalankan program dengan sendirinya maka digunakan untuk mengakses dan berinteraksi dengan komputer mainframe. Ada tiga jenis klien yang digunakan dalam konfigurasi klien diantaranya yaitu Thick, Thin dan Hybrid.
2. Server, mainframe yang menempati ruang besar dan harus melayani ratusan thin client di seluruh organisasi. Tugas utama server adalah menyediakan layanan dan sumber daya kepada kliennya, semakin besar jumlah aplikasi dan penggunaannya maka semakin banyak server yang didedikasikan untuk tujuan tertentu.
3. Azure, rangkaian layanan cloud yang membantu aktivitas organisasi, memberi kesempatan untuk dapat membangun, mengelola, dan menerapkan aplikasi jaringan secara global, membantu dalam melakukan konfigurasi dan pengelolaan klien dan server pada satu jaringan.



Perbedaan Otentifikasi dan Otorisasi

1. Network Otentifikasi

   Otentifikasi merupakan proses jaringan memisahkan akses yang sah dari yang lain atau yang mencurigakan. Sehingga otentifikasi jaringan melakukan konfigurasi untuk memverifikasi pengguna yang mereka klaim. Otentifikasi kata sandi adalah bentuk otentifikasi yang memasukkan nilai rahasia untuk mendapatkan akses ke jaringan.

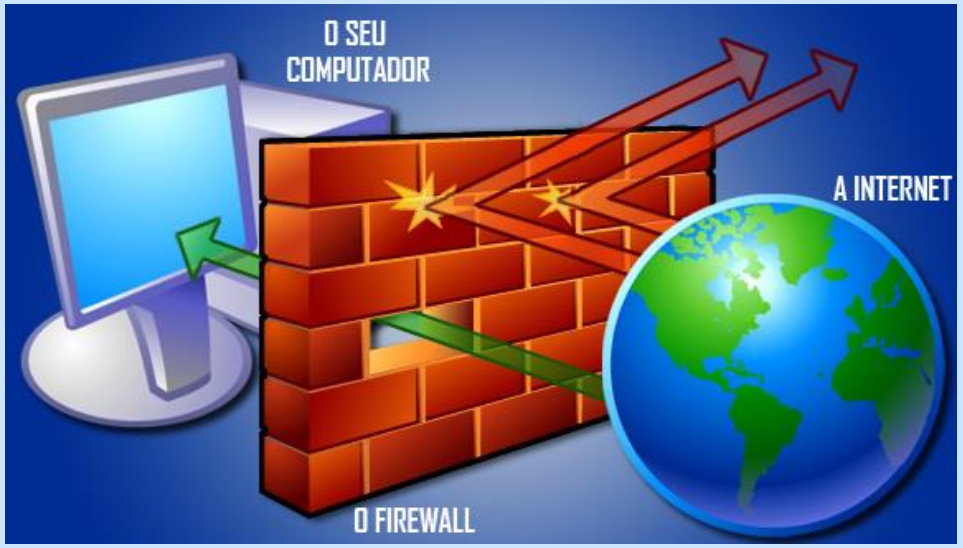
2. Network Otorisasi

   Ketika autentifikasi berhasil diselesaikan, kita harus memastikan bahwa pengguna atau klien yang diautentifikasi diberi otorisasi untuk dapat mengakses sumber daya atau layanan yang di inginkan. Izin tersebut dapat berupa membaca, menulis, atau menghapus, penggunaan izin tersebut haruslah tepat. Jangan pernah memberikan izin apa pun kepada pengguna atau klien yang tidak mereka perlukan.

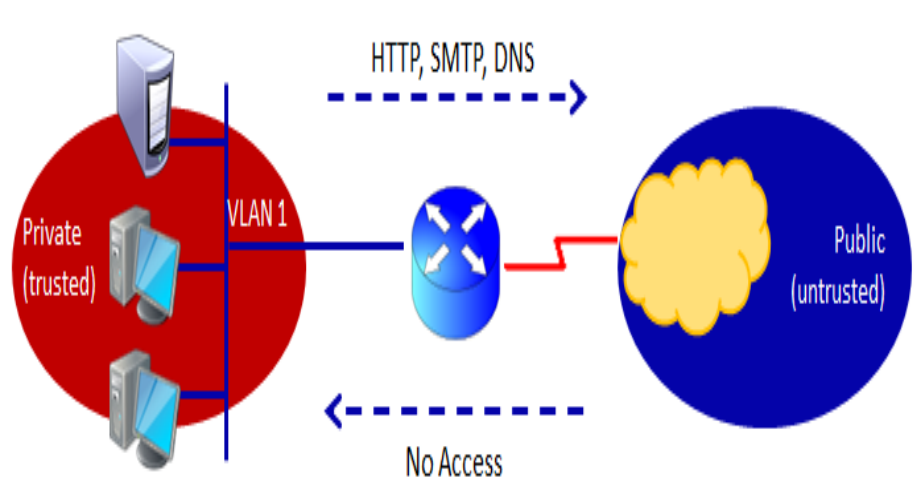
Berbagai Jenis Firewall di Jaringan Berbeda

Jaringan yang rentan dapat dieksploitasi oleh penyerang untuk mencuri informasi dan membuat layanan dan sumber daya tidak dapat diakses kembali sehingga menyebabkan kerugian reputasi dan finansial.

1. Access Control
2. Antimalware Tools
3. Email Security
4. Instruksi Deteksi dan Pencegahan
5. VPN
6. Web Security and Wireless Security
7. Firewall Types



Berbagai Jenis Item Memantau dalam Jaringan



Pemantauan jaringan berarti memantau semua komponen jaringan seperti router, server, firewall, dan sejenisnya untuk kinerja dan kesalahan secara terus – menerus dan menganalisis informasi yang dikumpulkan.

1. Pemantauan dengan Agen

   Agen akan memantau dan mengumpulkan informasi pada suatu perangkat dan dikirimkan informasi ke solusi pemantauan jaringan sesuai dengan penggunaannya.

2. Pemantauan tanpa Agen

   Agen tidak hanya diperuntukkan sebagai pemantau perangkat, pemantauan tanpa agen dapat membantu menghindari keharusan mengonfigurasi dan memelihara di perangkat.

3. Interval Pemantauan

   Menunjukkan bagaimana seseorang ingin mengumpulkan informasi di salah satu perangkat jaringan pengguna.

4. Protokol

   Protokol manajemen jaringan yang dapat digunakan seperti protokol manajemen jaringan sederhana (SNMP), instrumentasi manajemen windows (WMI), dan protokol pencatatan sistem (Syslog).

5. Zona Keamanan Jaringan

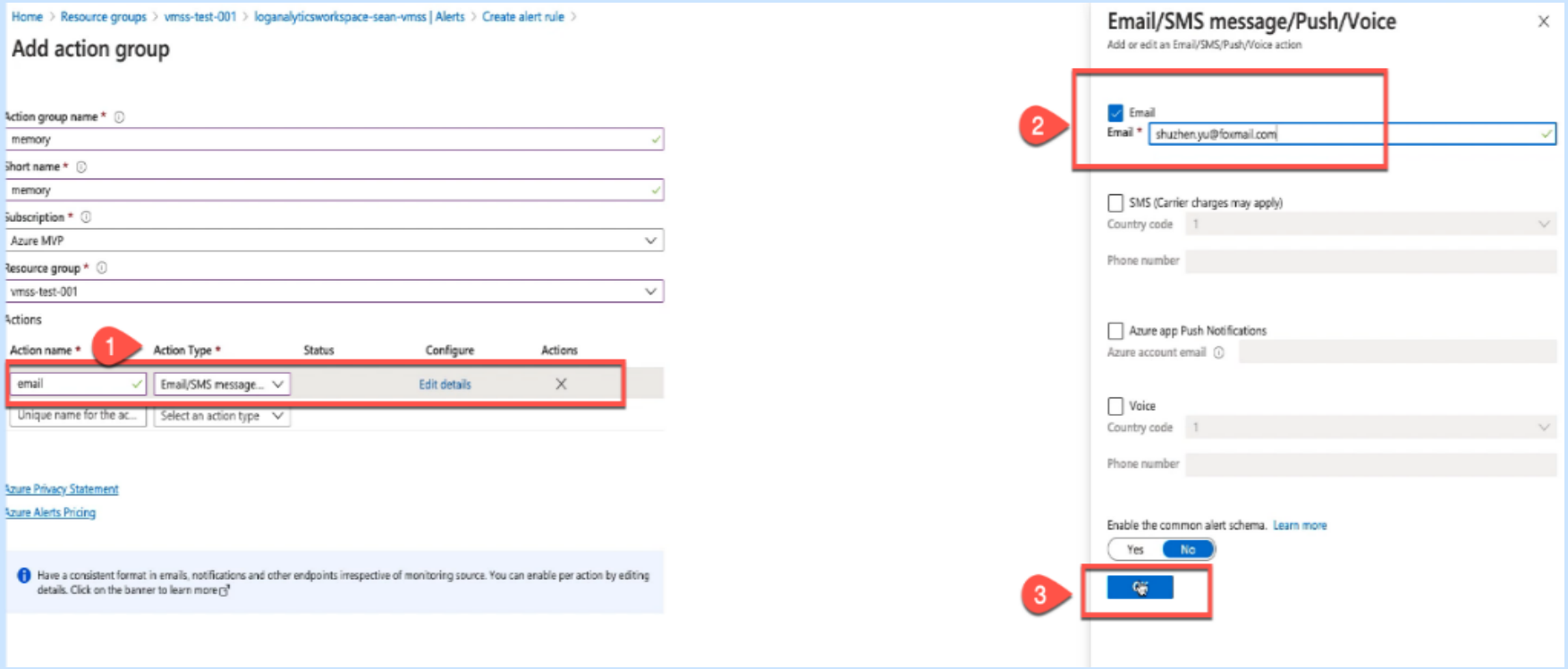
Cara Memetakan Komponen Jaringan Inti ke Jaringan Komputasi Awan

Mengelola sebuah jaringan akan menangani banyak tugas dan fungsi berbeda yang dikategorikan untuk membantu pelaksanaan secara efektif. Kategorinya dapat berupa manajemen kesalahan, manajemen konfigurasi, akuntasi/administrasi, manajemen kinerja dan keamanan (FCAPS).

1. Fault Management
2. Configuration Management
3. Accounting / Administration
4. Performance Management
5. Security

Beberapa solusi pemantauan jaringan Azure yang dapat kita gunakan untuk pelaporan dan peringatan

1. Azure Monitor, solusi pemersatu dengan mengumpulkan data log untuk di analisis sehingga mempermudah untuk mengambil tindakan yang tepat terhadap sumber daya di seluruh jaringan lokal dan Azure.



Beberapa solusi pemantauan jaringan Azure yang dapat kita gunakan untuk pelaporan dan peringatan

2. Log Analytics, digunakan untuk membuat kueri dan menggabungkan sejumlah besar data log untuk menganalisis komprehensif. Sehingga sangat membantu dalam mendapatkan pemahaman yang baik tentang sumber daya dan juga layanan di berbagai jaringan.


Thank You
See You Next
Chapter