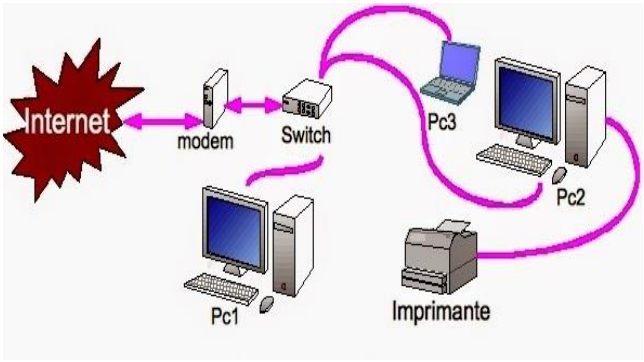
MODUL II

Dasar – Dasar Keamanan Jaringan

2.1 Model Jaringan Client - Server

Setelah mempelajari konsep dasar dari keamanan dunia internet, perlu dipahami juga apa sebenarnya jaringan itu. Jaringan sebagai salah satu atribut penghubung dan penyebab terjadinya ancaman dalam dunia internet. Jaringan adalah kumpulan perangkat yang mendukung untuk dapat berkomunikasi dalam kehidupan sehari – hari baik di rumah, tempat kerja, dan area publik.



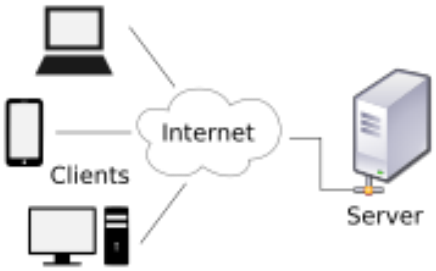
Model Jaringan Client - Server

Bagaimana jaringan tersebut bisa hadir dan dapat digunakan oleh pengguna? Karena adanya infrastruktur jaringan yang meliputi repeaters, hubs, bridge, switch, dan router. Semua perangkat akan bergantung pada kontrol akses media atau alamat protokol internet (IP) dalam mengirimkan data di jaringan. Repeaters digunakan ketika dua port perangkat memiliki jarak yang agak jauh untuk meregenerasi paket data dengan kekuatan aslinya secara perlahan – lahan. Bridges sendiri seperti artinya yaitu jembatan yang digunakan dalam meningkatkan kinerja jaringan dengan mengurangi lintasan jaringan yang tidak diperlukan hingga sampai ke tempat tujuan data. Lalu adanya hub sebagai penghubung untuk lebih dari satu perangkat serta menyusun tata letak beberapa port sebagai koneksi i/o antara hub dan perangkat jaringan. Switch digunakan untuk menggabungkan fungsi dari bridges dan hub dengan menggunakan alamat MAC perangkat jaringan untuk menentukan tujuan suatu data. Sehingga switch beroperasi mode dupleks penuh yaitu mengirim dan menerima data pada perangkat jaringan di saat yang bersamaan. Terakhir yaitu router menghubungkan jaringan dengan alamat tujuan yang berbeda dan dalam waktu yang bersamaan. Semua jaringan di bangun dengan prinsip yang sama.

2.1.1. Network Client

Network Client atau dapat kita sebut dengan klien jaringan adalah suatu perangkat komputer yang ringan sehingga tidak dapat menjalankan program dengan sendirinya maka digunakan untuk mengakses dan berinteraksi dengan komputer mainframe.

Dengan berjalannya waktu, kemajuan teknologi semakin mempermudah klient untuk secara langsung mewakili sistem hardware dan software berinteraksi melalui server yang dapat diakses melalui jaringan di berbagai tempat.



Network Client

Ada tiga jenis klien yang sering digunakan dalam konfigurasi klien server yaitu:

1. Thick, sangat umum digunakan di jaringan dan sering dikenal sebagai workstation karena dapat memproses dan menyimpan data secara lokal tanpa harus menggunakan server.
2. Thin, sering disebut sebagai terminat karena tidak dapat memproses dan menyimpan data secara lokal. Sehingga bergantung sepenuhnya pada server untuk menyediakan komputasi serta penyimpanan dan diwakili oleh aplikasi web untuk menampilkan informasi dari server.
3. Hybrid, penggabungan dari klien thick dan thin karena dapat melakukan pemrosesan data lokal secara terbatas namun tidak memiliki kemampuan dalam penyimpanan lokal. Contohnya yaitu perangkat yang merender konten dan menyimpan hasil di server.

Client	Penggunaan Penyimpanan Lokal	Penggunaan CPU
Thick	Yes	Yes
Thin	No	No
Hybrid	No	Yes

Network Client

2.1.2. Server

Server merupakan sistem perangkat lunak, perangkat keras atau keduanya. Server adalah 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.

Server

Server dan perangkat lunaknya akan memaparkan berbagai layanan dan fungsi ke klien jaringan. Sebuah server akan mendukung berbagai banyak klien yang terhubung dan menggunakan layanan dari beberapa server. Misalnya, penggunaan server media dalam mengambil gambar dan voice tetapi untuk menarik data agar dapat ditampilkan harus menggunakan server database. Server memiliki beberapa model klien untuk berkomunikasi dan berbagi data serta sumber daya dengan klientnya :

1. Respon permintaan, klien akan mengirimkan permintaan ke server lalu server akan melakukan aktivitas mengirimkan kembali tanggapan yang berupa hasil dari sebuah permintaan.
2. Peer to Peer (P2P), klien dapat meminta layanan misalnya file dari perangkat lain dalam sebuah jaringan dan sebaliknya karena P2P termasuk jaringan yang tidak terstruktur dalam penggunaan ad hoc.
3. Terbitkan dan berlangganan, klien akan berlangganan layanan di server. Ketika server menerima pesan baru maka akan dikirimkan respons ke setiap klien yang telah berlangganan.

Jaringan klien server termasuk jenis arsitektur jaringan yang sangat umum digunakan dan pastinya ada pro ataupun kontra dalam penggunaannya. Keuntungan sebuah client server dalam sebuah organisasi pastinya akan berkaitan dengan manajemen sumber daya dan keamanan, seperti semua pengguna akan dikelola secara terpusat dalam mengakses dan mengontrol ke server dan layanan, apabila arsitektur server dirancang untuk skala tertentu maka probabilitas penggunaan terjadinya masalah kinerja akan meningkat. Kemudian, semua data yang dimiliki oleh suatu organisasi dapat disimpan dan diakses secara terpusat sehingga mengurangi adanya duplikasi data, serta penjagaan data yang sangat terpusat ke media backup lainnya. Sama halnya dengan teknologi, pastinya client server memiliki bebrapa kekurangan diantaranya yaitu saat kegagalan sebuah server yang menyebabkan pengguna tidak dapat mengakses sumber daya yang terpusat sehingga akan mempengaruhi semua penggunanya. Dalam penyediaan arsitektur client server pastinya memerlukan perangkat lunak khusus dan perangkat keras tertentu yang memungkinkan price nya mahal dari yang lainnya. Lalu saat menjalankan dan memelihara jaringan dibutuhkan seseorang yang professional di bidang TI dengan beberapa permintaan khusus dalam sebuah operasi untuk meningkatkan kinerja suatu server.

2.1.3. Azure

Azure

Azure adalah rangkaian layanan cloud yang membantu aktivitas organisasi dalam memenuhi tantangan bisnis baik di waktu sekarang maupun waktu yang akan datang. Azure memberi kesempatan untuk dapat membangun, mengelola, dan menerapkan aplikasi jaringan secara global dengan menggunakan alat dan kerangka kerja sesuai ketentuan organisasi. Azure memiliki beberapa alat yang membantu dalam melakukan konfigurasi dan pengelolaan klien dan server pada satu jaringan.

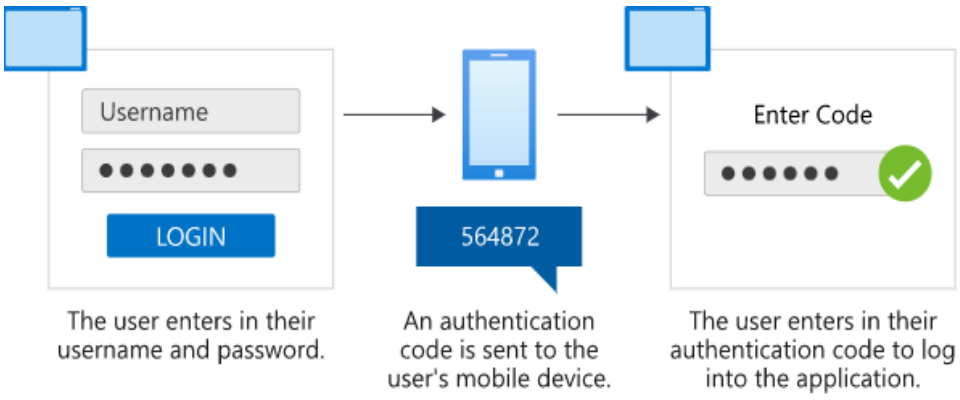
1. Manajer Sumber Daya Azure, layanan manajemen yang menyediakan sarana untuk mengatur serta mengamankan aset dan sumber daya suatu organisasi dengan menggunakan kontrol akses berbasis peran (RBAC) dalam meningkatkan keamanan dan akses ke asset dan sumber daya.
2. Mesin Virtual Azure, mengimplementasikan server tanpa perlu membeli dan memasang perangkat keras server. Virtualisasi memberikan fleksibilitas untuk beberapa server khusus dan lingkungan cloud. Azure VM akan bekerja dengan cloud dan jaringan lokal untuk memenuhi kebutuhan organisasi di saat sekarang dan akan datang.

2.2 Perbedaan Otentifikasi dan Otorisasi

Sumber daya jaringan seperti server dan aplikasi hanya dapat diakses oleh pengguna atau layanan yang terautentifikasi dan berwenang.

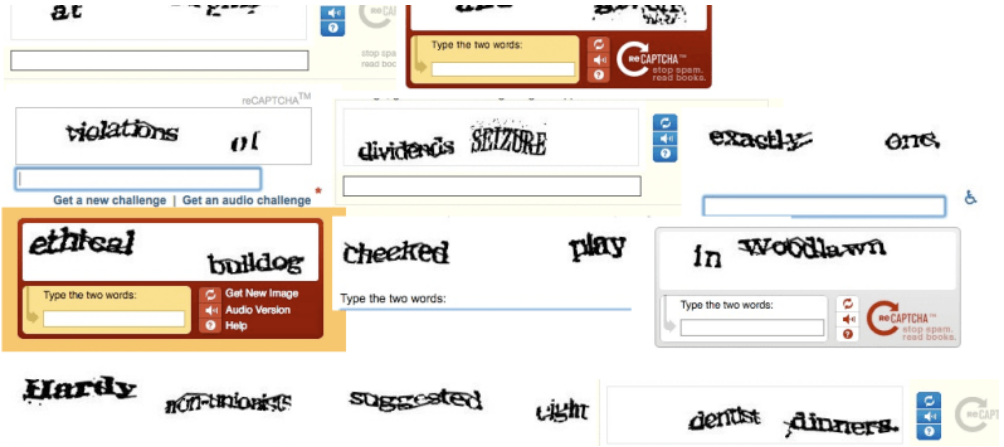
2.2.1 Network Otentifikasi

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. Kata sandi yang aman harus memenuhi kriteria yang ditentukan misalnya memiliki karakter huruf kapital, angka dan simbol. Ada dua faktor otentifikasi sebagai mekanisme yang memungkinkan pengguna untuk melakukan verifikasi. Misalnya, pengguna akan menerima kode melalui pesan teks atau kode yang dibuat melalui aplikasi di ponsel seperti Microsoft Authenticator.



Network Otentifikasi

Otentifikasi berbasis token menyerupai dengan otentifikasi dua faktor tersebut seperti penggunaan ponsel. Pada saat penggunaannya, para pengguna harus memastikan bahwa telah mengembalikan perangkat apabila tidak memerlukan akses kembali. Otentifikasi biometrik lebih ke penggunakan fisik seperti sidik jari, fitur wajah atau suara. Serta adanya otentifikasi transaksional untuk meneliti karakteristik pengguna misalnya mengharapkan para pengguna dapat mengakses jaringan secara teratur dari Amerika Serikat selama jam kerja. Akan tetapi, apabila ada akun pengguna yang masuk pada waktu tengah malam maka akan ditandai oleh sistem dan meminta pengguna untuk memverifikasi tambahan yang bertujuan untuk memberikan lapisan perlindungan tambahan untuk jaringan. Otentifikasi pengenalan komputer digunakan untuk mengakses jaringan, artinya pengguna hanya diizinkan masuk dari satu perangkat saja sehingga mempersulit pengguna apabila ingin berpindah perangkat. Sehingga diperlukan verifikasi yang membuktikan apakah entitas yang mencoba mengakses ke sistem tersebut adalah manusia dengan menggunakan tes *captcha* (Completely Automated Public Turing test to tell Computers and Humans Apart), tes tersebut akan menyajikan gambar scenario, huruf ataupun angka yang dikaburkan dan pengguna akan diminta untuk menjelaskan apa yang dilihat.



Network Otentifikasi

Selain tes captcha, sering kita dengar ada sistem *sso* (single sign on) yang menyediakan akses untuk mengautentifikasi pengguna dalam mengambil informasi identitas atau memperoleh titik aman lainnya.

2.2.2 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. Misalnya, pengguna database memiliki izin untuk mengakses dan membuat perubahan pada suatu database tetapi untuk database yang lain tidak dapat diakses oleh pengguna tersebut karena hanya database tertentu saja yang diperoleh izin. 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.

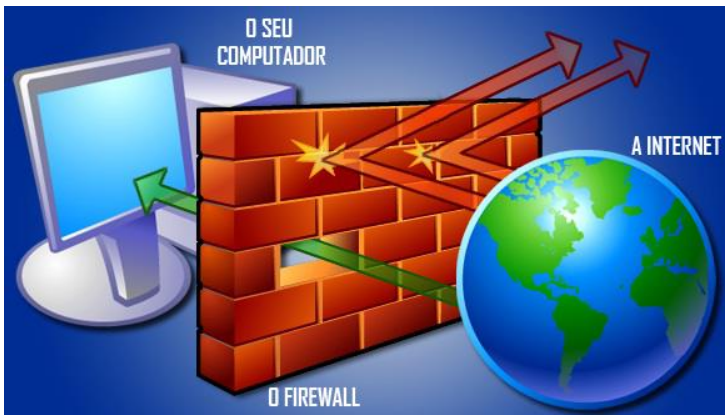
Perbedaan antara otentifikasi dan otorisasi dapat dilihat pada tabel di bawah ini.

Otentifikasi	Otorisasi
Mengonfirmasi apakah pengguna/klien yang melakukan klaim	Mengonfirmasi apakah pengguna/klien melakukan tindakan terhadap layanan
Meminta kredensial seperti nama pengguna dan kata sandi	Memeriksa izin yang dilampirkan ke akun dan izin yang dibutuhkan
Harus terjadi sebelum otorisasi	Terjadi setelah otentifikasi berhasil

Perbedaan Otentifikasi dan Otorisasi

2.3 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.



Berbagai Jenis Firewall di Jaringan Berbeda

Diperlukan keamanan yang kuat untuk mencegah kejadian mencurigakan berupa serangan dan kelemahan di jaringan. Di bawah ini akan di jelaskan berbagai jenis strategi keamanan jaringan yang dapat diterapkan.

2.3.1. Access Control

Kontrol akses dapat digunakan untuk memeriksa setiap pengguna dan klien untuk menentukan apakah memiliki izin untuk mengakses jaringan atau sumber daya. Kontrol akses tersebut dapat diimplementasikan dengan mengonfigurasi kebijakan keamanan yang memastikan pengguna memiliki izin yang tepat dan ditetapkan untuk melakukan tindakan tertentu di jaringan tersebut. Misalnya, menolak akses baca untuk beberapa sumber daya saat pengguna tersambung dari luar lokasi jaringan.

2.3.2. Antimalware Tools

Tools antimalware dapat melindungi jaringan yang digunakan dari malware (perangkat lunak berbahaya). Malware dapat berbentuk apa saja seperti trojan, virus, spyware, dan ransomware. Sehingga tools antimalware dan antivirus digunakan untuk memantau dan memperbaiki

malware, tool tersebut juga dapat mendeteksi anomali dalam sebuah file, menghapus potongan kode berbahaya, dan dapat memperbaiki sumber daya dan perangkat yang terpengaruh di jaringan tersebut.

2.3.3. Email Security

Email Security

Penyerang sering menggunakan email untuk mengakses jaringan pengguna. Email yang terlihat asli bisa saja meminta pengguna untuk membuka tautan dan memberikan detail yang digunakan penyerang agar dapat mengakses sumber daya jaringan pengguna. aplikasi email seperti Microsoft Outlook membantu untuk mengidentifikasi pesan dan pengirim yang mencurigakan.

2.3.4. Instrusion Detection and Prevention

Mendeteksi dan mencegah penyusupan dengan mengambil postur keamanan jaringan yang proaktif dan preventif sehingga pengguna dapat mengidentifikasi instrusi dan menggunakan alat pencegahan untuk memantau semua lalu lintas jaringan. Misalnya, Azure Network Watcher menyediakan data ke sistem deteksi instrusi sumber terbuka. Melalui sistem tersebut dapat dianalisis di Azure dan memperingatkan pengguna bahwa ada gangguan.

2.3.5. VPN

VPN

Virtual Private Network (VPN) dapat membuat koneksi terenkripsi dari satu jaringan ke jaringan lainnya melalui internet. VPN dapat mengonfigurasi terowongan terenkripsi untuk menyediakan komunikasi yang aman dan kemampuan akses jarak jauh di seluruh jaringan.

2.3.6. Web Security and Wireless Security

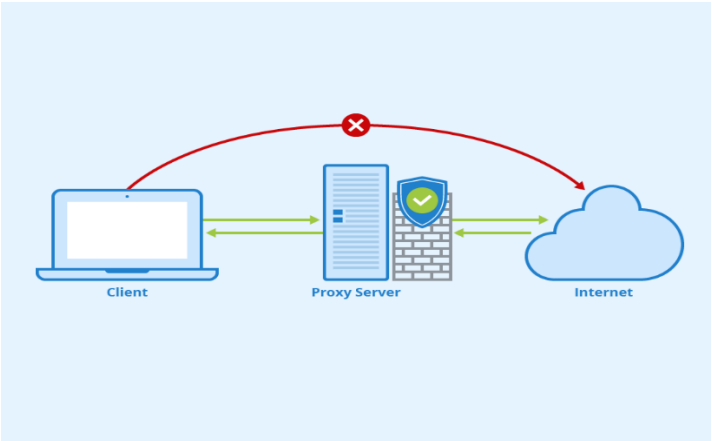
Pengguna dapat menggunakan fitur web untuk mencegah pengguna mengakses jenis situs tertentu yang telah ditandai warna merah. Alat keamanan web memungkinkan pengguna untuk mengatur kebijakan dalam memutuskan bagaimana pengguna menangani berbagai jenis permintaan web di jaringan. Jaringan nirkabel dapat diakses dari luar organisasi pengguna,

bergantung kepada kekuatan sinyal nirkabel. Langkah yang tepat untuk mengamankan jaringan nirkabel adalah dengan menggunakan jenis enkripsi terkuat yang tersedia pada perangkat nirkabel saat ini serta mengonfigurasi jaringan nirkabel yang terpisah untuk mencegah pengunjung menggunakan jaringan nirkabel yang ditujukan oleh pengguna internal.

2.3.7. Firewall Types

Jaringan firewall adalah alat keamanan yang memblokir atau memperbaiki akses tidak sah ke jaringan pengguna. Firewall dapat memantau dan membuat log dari semua lalu lintas di seluruh jaringan pengguna, sehingga dipergunakan kebijakan keamanan dalam mengonfigurasi firewall untuk mengambil tindakan yang sesuai pada semua lalu lintas jaringan. Firewall dapat berupa implementasi perangkat keras ataupun perangkat lunak. Perangkat keras yang dimaksud seperti perangkat fisik (contohnya router) yang berdiri sendiri atau bagian dari perangkat lain di jaringan pengguna. Firewall perangkat keras sangat mahal untuk dioperasikan dan biasanya ditemukan di berbagai organisasi besar. Sedangkan perangkat lunaknya dapat diinstal dan dikonfigurasi pada perangkat pengguna seperti workstation atau server. Firewall perangkat lunak memiliki fitur yang fleksibel dan dapat dijalankan di banyak perangkat dengan lebih hemat biaya. Firewall dapat melakukan beberapa fungsi berbeda di seluruh jaringan pengguna, yaitu :

1. Firewall lapisan aplikasi, berupa alat fisik atau berbasis perangkat lunak seperti filter atau plug-in.
2. Firewall pemfilteran paket, memeriksa setiap paket data saat melewati jaringan pengguna untuk menentukan apakah akan diblokir paket tertentu atau tidak.
3. Firewall tingkat sirkuit, memeriksa koneksi TCP dan UDP di seluruh jaringan pengguna valid sebelum datanya di pertukarkan.
4. Firewall server proxy, mengontrol informasi yang masuk dan keluar dari jaringan. Server proxy akan memberikan keselamatan dan keamanan dalam akses internet ke semua perangkat di jaringan pengguna.



Firewall Types

5. Firewall statefull, memeriksa karakteristik tentang koneksi di jaringan pengguna, memantau paket dari waktu ke waktu dan menyimpan kombinasi informasi pada sebuah tabel status. Apabila saat pencocokan paket tidak dikenali maka informasi pada tabel tersebut akan diblokir lalu lintasnya.
6. Firewall generasi berikutnya melakukan banyak fungsi sama halnya dengan firewall stateful. Namun cakupannya lebih luas dari jenis firewall lain seperti pemfilteran paket dan dukungan VPN. Firewall ini akan menyelidiki paket lebih teliti, misalnya dapat melihat muatan untuk setiap paket dan memeriksa karakteristik dan malware yang mencurigakan.

Firewall sangat penting dalam penggunaan jaringan, karena dapat melindungi jaringan pengguna dari dunia luar sehingga ada beberapa hal yang harus perlu diketahui untuk menyiapkan firewall diantaranya yaitu penyerang akan menggunakan malware dan memanfaatkan bandwidth pengguna, informasi pribadi atau sensitif dapat dicuri, dan sumber daya jaringan, perangkat atau sejenisnya dijadikan sebuah tebusan. Sehingga tempatkanlah firewall di antara jaringan pengguna dan koneksi luar agar tetap terjaga keamanan jaringan yang kuat.

2.4 Berbagai Jenis Item Memantau dalam Jaringan

Setiap organisasi pasti memiliki server, aplikasi, layanan dan tentu saj ada sebuah data yang berguna untuk memberikan layanan dan produk kepada pengguna atau pelanggan. Faktor yang paling penting lainnya yaitu memantau jaringan secara teratur apakah melindung aset dan sumber daya organisasi ataukah tidak. 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. Diperlukan juga pendekatan pencegahan terhadap suatu masalah yang akan meningkatkan ketersediaan jaringan, mengurangi waktu henti juga kegagalan.

2.4.1. Pemantauan dengan Agen

Solusi pemantauan jaringan seringkali berbasis agen, agen termasuk bagian dari sebuah perangkat lunak yang berjalan pada perangkat yang sedang di pantau. Agen akan memantau dan mengumpulkan informasi pada suatu perangkat dan dikirimkan informasi ke solusi pemantauan jaringan sesuai dengan penggunaannya. Agen juga akan membantu mengumpulkan data granular pada perangkat yang dipantau. Contohnya, agen dapat mengumpulkan informasi tentang proses yang berjalan pada suatu perangkat atau kinerja perangkat kerasnya. Perlu diketahui juga bahwa agen memerlukan waktu dalam menginstal dan mengkonfigurasi, belum lagi untuk proses pemeliharaan dan pembaruan yang akan memakan waktu jika memiliki banyak agen.

2.4.2. Pemantauan tanpa Agen

Agen tidak hanya diperuntukkan sebagai pemantau perangkat, pemantauan tanpa agen dapat membantu menghindari keharusan mengonfigurasi dan memelihara di perangkat. Namun, memungkinkan informasi yang di kumpulkan tidak sedetail ketika menggunakan pemantauan

dari seorang agen. Sehingga beberapa perangkat juga tidak dapat mengekspos informasi yang dibutuhkan.

2.4.3. Interval Pemantauan

Menunjukkan bagaimana seseorang ingin mengumpulkan informasi di salah satu perangkat jaringan pengguna. Frekuensi interval bergantung pada apa yang dipantau, misalnya akan menggunakan interval untuk memantau apakah perangkat tertentu tersedia atau tidak. Jikalau memantau penggunaan memori dan CPU pastinya dengan interval waktu beberapa menit, tidak perlu kita memantau setiap perangkat dengan interval yang singkat pada setiap matrik. Karena itu akan menambahkan beban yang tidak perlu ke jaringan.

2.4.4. Protocols

Ketika menggunakan sebuah koneksi jaringan, haruslah memperhatikan protokol jaringan mana yang digunakan agar tidak menggunakan bandwidth yang banyak. Ada beberapa protokol manajemen jaringan yang dapat digunakan, yaitu :

1. Protokol Manajemen Jaringan Sederhana (SNMP)

   Sama halnya switch juga router, agennya sudah diinstal sebelumnya pada suatu perangkat dan memungkinkan untuk konfigurasi. Agen harus mengumpulkan beberapa hal seperti lintasan pada sakelar jaringan, penggunaan memori dan antrian printer. Protokol ini akan mengkomunikasikan informasi tentang perangkat ke solusi pemantauan dan manajemen jaringan (NMS).
2. Instrumentasi Manajemen Windows (WMI)

   Perangkat Windows menggunakan protokol ini untuk memberikan informasi suatu perangkat. Kegunaan lainnya yaitu dapat membuat perubahan perangkat berupa penjadwalan, pembaruan dan pengaturan terhadap sistemnya. Infrastruktur manajemen windows memiliki kemampuan yang selalu ditingkatkan dengan integrasi yang lebih baik baik dengan powershell untuk melakukan perintah dan skrip.
3. Protokol Pencatatan Sistem (Syslog)

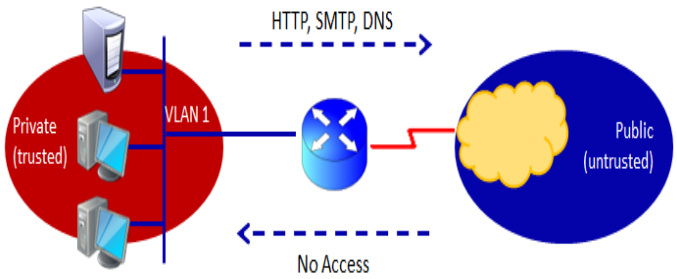
   Protokol yang memungkinkan perangkat mengirimkan catatan peristiwa. Misalnya, server web dapat menggunakan syslog untuk mencatat peristiwa tentang upaya yang gagal saat mengaksesnya atau router mencatat aktivitas pengguna.

2.4.5. Zona Keamanan Jaringan

Zona keamanan jaringan adalah pembagian penerapan kebijakan keamanan secara khusus dan dipisahkan dari segmen jaringan lain oleh firewall. Sehingg ada tiga jenis zona keamanan yang berbeda, yaitu :

1. Zona tepercaya atau sifatnya pribadi berisi sumber daya jaringan dan perangkat yang tidak diizinkan mengakses yang berada di luar organisasi. Contohnya seperti printer, workstation

yang digunakan oleh pengguna internal serta server internal. Sehingga di zona ini yang dilakukan adalah mengonfigurasi perangkat dengan alamat IP pribadi.



Zona Keamanan **Jaringan**

2. Zona publik berisi segala sesuatu di luar organisasi dapat berupa bagian dari internet atau jaringan lain namun tidak berada dalam kendali organisasi.
3. Jaringan perimeter atau zona demilierisasi adalah zona dengan sumber daya dan layanan yang dapat diakses dari luar ogranisasi yang tersedia. Contohnya menyediakan akses ke aplikasi, organisasi mitra dan pemasok.
4. Zona kebijakan pemfilteran yang menangani arus lalu lintas saat melewati zona yang berbeda. Kebijakan pemfilteran yaitu :
   a. Inside to outside dan inside to perimeter network, memeriksa semua lintasan yang berasal dan menuju ke jaringan perimeter. Contohnya, anggota staf internal ingin mengakses situs web publk, maka lintasan akan diperiksa apakah situs web tersebut dapat dipercaya atau tidak.
   b. Outside to inside, memblokir lintasan yang datang dari luar ke jaringan. Karena hanya ada satu lintasan yang diizinkan yaitu lintasan yang merupaj tanggapan secara langsung terhadap permintaan yang berasal dari zona dalam. Contohnya, anggota staf internal meminta halaman web dari sebuah server dan responsnya diizinkan.
   c. Outside to perimeter network, memeriksa semua lalu lintas yang datang dari luar dan menuju jaringan perimeter. Lintasan yang diizinkan yang masuk melewati lintas Email dan HTTPS.
   d. Perimeter ke jaringan luar, memeriksa lintasan yang berasal dari jaringan perimeter dimana diizinkan untuk bepergian ke luar jaringan berdasarkan aturan firewall dan sumber daya atau klien yang melakukan permintaan.

2.5 Cara Memetakan Komponen Jaringan Inti ke Jaringan Komputasi Awan

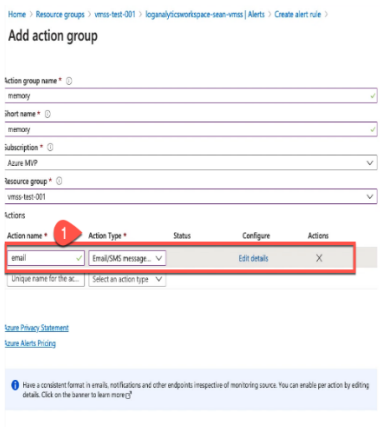
Saat mengelola sebuah jaringan pastinya akan menangani banyak tugas dan fungsi berbeda yang telah dikategorikan untuk membantu pelaksanaan secara efektif. Kategorinya dapat berupa manajemen kesalahan, manajemen konfigurasi, akuntasi/administrasi, manajemen kinerja dan

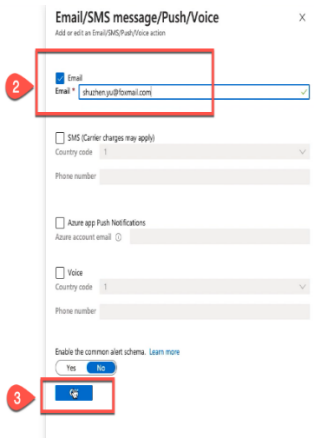
keamanan atau dapat dipersingkat menjadi FCAPS apabila menggunakan pelafalan bahasa inggris.

1. *Fault Management*, berkaitan dengan proses dan tugas yang digunakan untuk mengidentifikasi dan menyelesaikan kesalahan pada suatu jaringan.
2. *Configuration Management,* mencakup aspek pengumpulan informasi yang berdasarkan perubahan konfigurasi perangkat, perubahan perangkat keras fisik dan jaringan serta pembaruan perangkat lunak.
3. *Accounting / Administration,* mencakup jaringan yang digunakan dalam pengaturan penyedia layanan sehingga memerlukan pantauan dalam melacak pemanfaatan serta penagihan bagi pengguna. Apabila jaringan tidak berada dalam pengaturan penyedia layanan, maka administrasi serta tugas seperti mengelola izin juga kata sandi pengguna disertakan.
4. *Performance Management,* mencakup pengelolaan kinerja suatu jaringan seperti aspek pemantauan throughput, pemantauan pengguna serta peningkatan waktu respons.
5. *Security,* mencakup tugas yang dilakukan dalam mengamankan jaringan seperti melindungi perangkat, membatasi akses ke sumber daya jaringan serta melindungi aktivitas pengguna dalam suatu jaringan.

Saat kita memantau sebuah jaringan, pastinya kita akan mengumpulkan data dan memprosesnya untuk dimasukkan ke dalam sebuah format yang telah ditentukan untuk membuat keputusan manajemen yang tepat. Sehingga ada beberapa solusi pemantauan jaringan Azure yang dapat kita gunakan untuk pelaporan dan peringatan, diantaranya yaitu

a. 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. Azure monitor bervariasi dalam cakupan kemampuannya. Misalnya, Azure monitor menggunakan integrasinya untuk memeriksa dan mendiagnosis risiko dan masalah apa saja yang ada dalam sebuah aplikasi. Penggunaan Azure monitor yaitu untuk memberitahu tentang potensi masalah sehingga membantu saat mengambil tindakan lebih lanjut, serta memperbaiki potensi masalah.





Cara Memetakan Komponen Jaringan Inti ke Jaringan Komputasi Awan

b. 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.

Cara Memetakan Komponen Jaringan Inti ke Jaringan Komputasi Awan

DAFTAR PUSTAKA

Fundamentals of network security - Learn | Microsoft Docs

Network types and topologies to use when you design a network - Learn | Microsoft Docs

What is Azure VPN Gateway? - Learn | Microsoft Docs