Summary pertemuan 1 PKL IPB

Layer OSI 1-4

1. **Layer Physical**

Ini adalah layer yang paling sederhana; berkaitan dengan electrical (dan optical) koneksi antar peralatan. Data biner dikodekan dalam bentuk yang dapat ditransmisi melalui media jaringan, sebagai contoh kabel, transceiver dan konektor yang berkaitan dengan layer Physical.

Fungsi Physical Layer adalah Bertanggung jawab atas proses data menjadi bit dan mentransfernya melalui media, seperti kabel, dan menjaga koneksi fisik antar sistem.

Contoh device:

- Repeater
- Multiplexer
- Hubs(Passive and Active)
- TDR
- Oscilloscope
- Amplifier

2. **Layer Data-link**

Layer ini menyediakan transfer data yang lebih nyata. Sebagai penghubung antara media network dan layer protocol yang lebih high-level

Fungsi :

- Mengkomuninasikan bit ke bytes dan byte ke frame
- Menerima perangkat media berupa MAC Addressing
- Deteksi error dan recovery error
- Menyediakan transmisi phisik dari data
- Menangani notifikasi error, topologi jaringan, flow control
- Memastikan pesan-pesan akan terkirim melalui alat yang sesuai di LAN menggunakan hardware address (MAC)
- Media Access Control (MAC), 24 bit vendor code dan 24
- bit serial numbernya
-

Contoh device:

- Bridge
- Switch
- ISDN Router
- Intelligent Hub
- NIC
- Advanced Cable Tester

3. Layer Network

Tugas utama dari layer network adalah menyediakan fungsi routing sehingga paket dapat dikirim keluar dari segment network lokal ke suatu tujuan yang berada pada suatu network lain. IP, Internet Protocol, umumnya digunakan untuk tugas ini. Protocol lainnya seperti IPX, Internet Packet eXchange. Beberapa fungsi yang mungkin dilakukan oleh Layer Network

- Membagi aliran data biner ke paket diskrit dengan panjang tertentu
- Mendeteksi Error
- Memperbaiki error dengan mengirim ulang paket yang rusak
- Mengendalikan aliran

Contoh device:

- Brouter
- Router
- Frame Relay Device
- ATM Switch
- Advanced Cable Tester

4. Layer Transport

Layer transport data, menggunakan protocol seperti UDP, TCP dan/atau SPX (Sequence Packet eXchange, yang satu ini digunakan oleh NetWare, tetapi khusus untuk koneksi berorientasi IPX). Layer transport adalah pusat dari mode-OSI. Layer ini menyediakan transfer yang reliable dan transparan antara kedua titik akhir, layer ini juga menyediakan multiplexing, kendali aliran dan pemeriksaan error serta memperbaikinya.

- Melakukan segmentasi dan menyatukan kembali data yang tersegmentasi (reassembling) dari upper layer menjadi sebuah arus data yang sama.
- Menyediakan layanan tranportasi data ujung ke ujung.
- Membuat sebuah koneksi logikal antara host pengirim dan tujuan pada sebuah internetwork
- Bertanggung jawab menyediakan mekanismemultiplexing
- Multiplexing = teknik untuk mengirimkan danmenerima beberapa jenis data yang berbeda sekaligus pada saat yang bersamaan melaluisebuah media network saja.

Contoh device:

- Gateway
- Advanced Cable Tester
- Brouter

Software Defined Data Network

Software Defined Network (SDN) merupakan arsitektur jaringan yang bekerja dibawah kendali software sebagai kontrol utama. Dalam SDN, dilakukan pemisahan data dan control plane. Pemisahan ini mendefinisikan perangkat switch/router yang berada pada data plane secara sederhana menjadi perangkat *forwarding paket data* dan memberikan tangung jawab kepada software tertentu pada *control plane* sebagai controller yang secara logis terpusat untuk mengontrol perilaku seluruh jaringan. Kontroler merupakan bagian yang sangat vital pada arsitektur SDN. Karena kontroler lah yang akan mendefinisikan jaringan, mengatur masalah availability, laju traffic data, routing & forwarding dll. Kontroler yang meng-handle seluruh infrastuktur jaringan yang ada dibawahnya.

Kontroler sendiri merupakan sebuah perangkat lunak yang dapat dikembangkan sesuai kebutuhan jaringan. Banyak vendor-vendor yang telah menciptakan kontroler. Kontroler-kontroler tersebut diantaranya:

1. POX
2. NOX
3. Floodlight
4. Pyretic
5. Beacon
6. Ryu
7. OpenDay Light

Kontroler-kontroler tersebut memiliki basis bahasa pemrograman yang berbeda-beda. Ada yang menggunakan C++, Python, hingga Java.

Beberapa aspek penting dari SDN adalah :

1. Adanya pemisahan secara fisik/eksplisit antara *forwarding/data-plane* dan *control-plane*
2. Antarmuka standard (*vendor-agnosic*) untuk memprogram perangkat jaringan
3. *Control-plane* yang terpusat (secara logika) atau adanya sistem operasi jaringan yang mampu membentuk peta logika (*logical map*) dari seluruh jaringan dan kemudian memrepresentasikannya melalui (sejenis) API (*Application Programming Interface*)
4. Virtualisasi dimana beberapa sistem operasi jaringan dapat mengkontrol bagian-bagian (*slices* atau *substrates*) dari perangkat yang sama.

Arsitektur jaringan tradisional saat ini kompleksitasnya semakin lama semakin tinggi. Pertukaran informasi antar router akan semakin komplek jika pertumbuhan jaringannya semakin besar. Oleh karena itu SDN diciptakan untuk mengatasi kompleksitas-kompleksitas yang terjadi pada arsitektur jaringan tradisional.

Sehingga dapat disimpulkan bahwa alasan diciptakannya SDN adalah untuk inovasi dan juga beberapa hal berikut:

1. Virtualisasi dan Cloud: Komponen dan entitas jaringan hybrid - antara fisik bare metal dan yg virtual.
2. Orchestration dan Scalability: Kemampuan untuk mengatur dan mengelola ribuan perangkat melalui sebuah point of management.
3. Programmability dan Automation: Kemampuan untuk mengubah behaviour (perilaku) jaringan serta untuk dapat melakukan perubahan terebut secara otomatis (sebagai contoh adalah kemampuan troubleshooting, perubahan policy dan lain-lain).
4. Visibility: Kemampuan untuk dapat memonitor jaringan, baik dari sisi sumber daya, konektivitas dan lain-lain.
5. Kinerja: Kemampuan untuk memaksimalkan penggunaan perangkat jaringan, misalnya optimasi bandwidth, load balancing, traffic engineering dan lain-lain (berhubungan dengan Programmability dan Scalability).

Arsitektur SDN dapat dilihat sebagai 3 lapis/bidang:

1. infrastruktur (data-plane / infrastructure layer): terdiri dari elemen jaringan yg dapat mengatur SDN Datapath sesuai dengan instruksi yg diberikan melalui Control-Data-Plane Interface (CDPI).
2. kontrol (control plane / layer): entitas kontrol (SDN Controller) mentranslasikan kebutuhan aplikasi dengan infrastruktur dengan memberikan instruksi yg sesuai untuk SDN Datapath serta memberikan informasi yg relevan dan dibutuhkan oleh SDN Application.
3. aplikasi (application plane / layer): berada pada lapis teratas, berkomunikasi dengan sistem via NorthBound Interface (NBI).

Bidang Management & Admin bertanggung-jawab dalam: inisiasi elemen jaringan, memasangkan SDN Data path dengan SDN Controller, atau menkonfigurasi cakupan (coverage) dari SDN Controller dan SDN App.

Menurut Shenker, SDN control plane memerlukan setidaknya 3 jenis abstraksi (SDN v1 & v2) :

1. Forwarding Abstraction : bertujuan untuk menjadikan mekanisme forwarding yg fleksibel dan tidak bergantung pada jenis perangkat (vendor neutrality).
2. State Distribution Abstraction : bertujuan untuk medapatkan global network view dan menangani semua proses state dissemination/collection. Abstraksi ini dilakukan oleh NOS (Network Operating System) yg merupakan sistem terdistribusi, berkomunikasi dengan elemen jaringan untuk membuat network view. Aplikasi/control-program menggunakan network-view ini untuk menghasilkan konfigurasi setiap elemen jaringan.
3. Specification Abstraction : bertujuan untuk mendapatkan abstract network view yg merupakan fungsi dari global network view. Abstraksi ini dilakukan oleh Network Hypervisor (Nypervisor) yg menterjemahkan abstract ke global network view. Dengan Nypervisor, aplikasi/control-programdapat berinteraksi dengan jaringan seolah-olah seperti single-device.

Dalam istilah Shenker, SDN v1 adalah gabungan antara NOS dengan abstraksi forwarding. SDN v2 sudah termasuk Network Hypervisor.

Sering ada yg keliru beranggapan bahwa OpenFlow (OF) adalah sinonim SDN. OpenFlow hanya merupakan salah satu komponen dari arsitektur SDN. OF merupakan pionir standard terbuka untuk protokol komunikasi antara *control* dan *forwarding plane* (i.e. *Southbound* APIs).

Software Defined Data Center

SDDC (Software Define Data Center) atau juga dikenal disebut dengan VDC (Virtual Data Center) adalah teknologi data center yang menggunakan teknologi virtualisasi untuk membagi infrastruktur perangkat keras ke dalam mesin-mesin virtual, sehingga penyedia layanan (service provider) dapat menyediakan layanan jaringan dan komputasi kepada client-client yang berbeda. Infrastruktur perangkat keras (hardware) yang dapat dimasukkan ke dalam mesing-mesin virtual di sini yaitu: Networking, storage, CPU, dan Security. Proses penyediaan, penyeberan, pengoperasian dari seluruh infrastruktur hardware tersebut diimplementasikan melalui perangkat lunak (software).

SDDC sangat membantu perusahaan untuk dapat menekan investasi infrastruktur, SDM dan energi. Kemudahan pengoperasian yang tidak harus membutuhkan SDM ahli di bidang networking, storage, maupun security menjadi salah satu keuntungan dari penerapan SDDC ini. Software virtualisasi yang bisa digunakan yaitu VMware. SDDC saat ini lebih merupakan konsep daripada praktik yang umum diterapkan, namun telah melihat adopsi bertahap oleh penyedia layanan cloud dan penyedia layanan data-center-as-a-service. Daftar ini mencakup Amazon, Google dan Open Compute Project.

Ada tiga blok utama SDDC, yaitu :

- Virtualisasi network menggabungkan sumber daya jaringan dengan membagi bandwidth yang tersedia ke saluran independen yang masing-masing dapat ditugaskan atau ditugaskan kembali ke server atau perangkat tertentu secara real time.
- Virtualisasi storage melakukan penyimpanan fisik dari beberapa perangkat penyimpanan jaringan ke dalam perangkat penyimpanan tunggal yang dikelola dari central console.
- Virtualisasi server pada sumber daya server, termasuk jumlah dan identitas server fisik individu, Processors dan Operating System (OSes), dari pengguna server. Maksudnya adalah untuk meluangkan pengguna dari pengelolaan rincian sumber daya server yang

rumit, ini juga meningkatkan pembagian dan pemanfaatan sumber daya, sambil mempertahankan kemampuan untuk memperluas kapasitas di kemudian hari.

SDDC yang didefinisikan perangkat lunak adalah cara untuk mengkonfigurasi dan menyediakan aplikasi, infrastruktur, dan sumber daya secara dinamis. Desainnya memungkinkan data center dikelola sebagai sistem terpadu atau gabungan kumpulan domain. Faktor kunci adalah pemisahan bidang kontrol dan bidang data. SDDC menyediakan sebuah organisasi dengan cloud pribadinya untuk mendapatkan data host yang lebih baik.

SDDC yang didefinisikan perangkat lunak memanfaatkan ketangkasan, elastisitas dan skalabilitas komputasi cloud. Keuntungan utama adalah mengotomatisasi semua fungsi melalui perangkat lunak cerdas, terutama tugas intensif secara manual yang berkaitan dengan penyediaan dan manajemen operasional. Hal ini memungkinkan fleksibilitas tingkat tinggi dalam pusat data tradisional. Sumber daya dikumpulkan dan tersedia dengan cara cloud pribadi atau cloud hibrida. Beban kerja beroperasi secara independen dari infrastruktur TI fisik. Manajemen infrastruktur dan manajemen beban kerja dikendalikan secara terprogram. Hasil yang diharapkan adalah mengurangi overhead biaya dan manajemen. SDDC terdiri dari komponen yang berbeda dari berbagai vendor. Itu mempersulit perencanaan dan integrasi arsitektur SDDC, walaupun perusahaan dapat menghindari vendor lock-in sebagai hasilnya.

Keuntungan dari SDDC untuk klien adalah mereka tidak perlu membangun infrastruktur. Jika mereka membutuhkan sumber daya komputasi, jaringan, dan penyimpanan, mereka hanya bisa "menyewakan" mereka melalui cloud. Keuntungan untuk perangkat lunak atau penyedia layanan adalah mereka dapat menggunakan infrastruktur data center terpusat untuk melayani banyak klien. Salah satu unsur yang telah mendorong pertumbuhan SDDC dan komputasi cloud pada umumnya adalah biaya perangkat keras dan penyimpanan yang merosot. Karena sumber daya ini semakin murah, akan lebih ekonomis untuk membangun pusat data yang besar dalam skala besar dan kemudian menjual sumber daya ini sebagai Infrastructure as a Service (IAAS).

Komponen SDDC mencakup elemen jaringan yang didefinisikan perangkat lunak (SDN), perangkat lunak yang didefinisikan penyimpanan, dan mesin virtual, atau komputasi virtual. Banyak platform perangkat lunak yang berbeda - terbuka dan eksklusif - dapat digunakan untuk virtualisasi sumber daya komputasi, termasuk Citirix, KVM, OpenDaylight, OpenStack, OpenFlow, Red Hat, dan VMware di antara banyak lainnya.

Software Defined Cloud Computing

Software defined cloud computing (SDCC) berkembang sebagai paradigma komputasi utilitas yang berhasil untuk *Information and Communication Technology* (ICT) dalam hal pengiriman sumber daya sebagai layanan melalui Internet. Penggunaan *cloud computing* menyangkup bidang industri, pemerintah hingga akademis. Cloud Computing adalah suatu paradigma di mana informasi secara permanen tersimpan di server di internet dan tersimpan secara sementara di komputer pengguna (client) termasuk di dalamnya adalah desktop, komputer tablet, notebook, komputer tembok, handheld, sensor-sensor, monitor dan lain-lain

Dengan bertambahnya adopsi *cloud*, jumlah *cloud providers* dan *services* juga meningkat. Ratusan penyedia layanan menawarkan salah satu dari tiga layanan, yaitu Software as a Service (SaaS), Platform as a Service (PaaS), dan Infrastructure as a Service (IaaS). Selanjutnya, terdapat beragam produk yang ditawarkan oleh masing-masing *provider* untuk setiap model layanan, dan setiap produk dapat dikonfigurasi dengan banyak parameter yang berbeda. Berbagai layanan ini menciptakan tantangan untuk penyedia layanan untuk menerapkan Service Level Agreements (SLAs) yang menyatakan Quality of Service (QoS).

- Infrastructure as a Service (IaaS)

  Infrastructure as a Service adalah layanan komputasi cloud yang menyediakan infrastruktur IT berupa CPU, RAM, storage, bandwith dan konfigurasi lain. Komponen-komponen tersebut digunakan untuk membangun komputer virtual. Komputer virtual dapat diinstal sistem operasi dan aplikasi sesuai kebutuhan. Keuntungan layanan IaaS ini adalah tidak perlu membeli komputer fisik sehingga lebih menghemat biaya. Konfigurasi komputer virtual juga bisa diubah sesuai kebutuhan. Misalkan saat storage hampir penuh, storage bisa ditambah dengan segera. Perusahaan yang menyediakan IaaS adalah Amazon EC2, TelkomCloud dan BizNetCloud.
- Platform as a Service (PaaS)

  Platform as a Service adalah layanan yang menyediakan computing platform. Biasanya sudah terdapat sistem operasi, database, web server dan framework aplikasi agar dapat menjalankan aplikasi yang telah dibuat. Perusahaan yang menyediakan layanan tersebutlah yang bertanggung jawab dalam pemeliharaan computing platform ini. Keuntungan layanan PaaS ini bagi pengembang adalah mereka bisa fokus pada aplikasi yang mereka buat tanpa memikirkan tentang pemeliharaan dari computing platform. Contoh penyedia layanan PaaS adalah Amazon Web Service dan Windows Azure.
- Software as a Service (SaaS)

  Software as a Service adalah layanan komputasi cloud dimana kita bisa langsung menggunakan aplikasi yang telah disediakan. Penyedia layanan mengelola infrastruktur dan platform yang menjalankan aplikasi tersebut. Contoh layanan aplikasi email yaitu gmail, yahoo dan outlook sedangkan contoh aplikasi media sosial adalah twitter, facebook dan google+. Keuntungan dari layanan ini adalah pengguna tidak perlu membeli lisensi untuk mengakses aplikasi tersebut. Pengguna hanya membutuhkan perangkat klien komputasi cloud yang terhubung ke internet. Ada juga

aplikasi yang mengharuskan pengguna untuk berlangganan agar bisa mengakses aplikasi yaitu Office 365 dan Adobe Creative Cloud.

Metode komputasi cloud

Berikut merupakan cara kerja penyimpanan data dan replikasi data pada pemanfaatan teknologi cloud computing. Dengan Cloud Computing komputer lokal tidak lagi harus menjalankan pekerjaan komputasi berat untuk menjalankan aplikasi yang dibutuhkan, tidak perlu menginstal sebuah paket perangkat lunak untuk setiap komputer, kita hanya melakukan installasi operating system pada satu aplikasi[8]. Jaringan komputer yang membentuk cloud (internet) menangani mereka sebagai gantinya. Server ini yang akan menjalankan semuanya aplikasi mulai dari e-mail, pengolah kata, sampai program analisis data yang kompleks. Ketika pengguna mengakses cloud (internet) untuk sebuah website populer, banyak hal yang bisa terjadi. Pengguna Internet Protokol (IP) misalnya dapat digunakan untuk menetapkan dimana pengguna berada (geolocation). Domain Name System (DNS) jasa kemudian dapat mengarahkan pengguna ke sebuah cluster server yang dekat dengan pengguna sehingga situs bisa diakses dengan cepat dan dalam bahasa lokal mereka. Pengguna tidak login ke server, tetapi mereka login ke layanan mereka menggunakan id sesi atau cookie yang telah didapatkan yang disimpan dalam browser mereka. Apa yang user lihat pada browser biasanya datang dari web server. Webservers menjalankan perangkat lunak dan menyajikan pengguna dengan cara interface yang digunakan untuk mengumpulkan perintah atau instruksi dari pengguna (klik, mengetik, upload dan lain-lain) Perintah-perintah ini kemudian diinterpretasikan oleh webservers atau diproses oleh server aplikasi. Informasi kemudian disimpan pada atau diambil dari database server atau file server dan pengguna kemudian disajikan dengan halaman yang telah diperbarui. Data di beberapa server disinkronisasikan di seluruh dunia untuk akses global cepat dan juga untuk mencegah kehilangan data

Web service telah memberikan mekanisme umum untuk pengiriman layanan, hal ini membuat service-oriented architecture (SOA) ideal untuk diterapkan. Tujuan dari SOA adalah untuk mengatasi persyaratan yang bebas digabungkan, berbasis standar, dan protocol-independent distributed computing. Dalam SOA, sumber daya perangkat lunak yang dikemas sebagai "layanan," yang terdefinisi dengan baik, modul mandiri yang menyediakan fungsionalitas bisnis standar dan konteks jasa lainnya. Kematangan web service telah memungkinkan penciptaan layanan yang kuat yang dapat diakses berdasarkan permintaan, dengan cara yang seragam.

Implementasi Komputasi cloud :

Ada tiga poin utama yang diperlukan dalam implementasi cloud computing, yaitu :

- **Computer front end**

Biasanya merupakan computer desktop biasa.

- **Computer back end**

Computer back end dalam skala besar biasanya berupa server computer yang dilengkapi dengan data center dalam rak-rak besar. Pada umumnya computer back end harus

mempunyai kinerja yang tinggi, karena harus melayani mungkin hinggga ribuan permintaan data.

- **Penghubung antara keduanya**

Penghubung keduanya bisa berupa jaringan LAN atau internet.

contoh computing cloud :

- Google Drive

Google Drive adalah layanan penyimpanan Online yang dimiliki Google. Google Drive diluncurkan pada tanggal 24 April 2012. Sebenarnya Google Drive merupakan pengembangan dari Google Docs. Google Drive memberikan kapasitas penyimpanan sebesar 5GB kepada setiap penggunanya. Kapasitas tersebut dapat ditambahkan dengan melakukan pembayaran atau pembelian Storage. Penyimpanan file di Google Drive dapat memudahkan pemilik file dapat mengakses file tersebut kapanpun dan dimanapun dengan menggunakan komputer desktop, laptop, komputer tablet ataupun smartphone. File tersebut juga dapat dengan mudah dibagikan dengan orang lain untuk berbagi pakai ataupun melakukan kolaborasi dalam pengeditan.

Fitur-fitur Google Drive

- **Penyimpanan gratis sebesar 5GB**

Google Drive memberikan fasilitas penyimpanan sebesar 5GB kepada penggunanya dengan cuma-cuma untuk menyimpan dokumen, baik berupa gambar, video, musik, ataupun file-file lain.

- **Memungkinkan membuat dokumen**

Pada fitur ini Google Drive memungkinkan para penggunanya untuk membuat dokumen, seperti mengolah data, mengolah angka, membuat presentasi, form dan dokumen lainnya.

- **Berbagi file**

Google Drive memudahkan untuk berbagi file dengan orang lain, dan juga memudahkan orang lain untuk melakukan pengeditan terhadap file yang kita buat.

- **Terintegrasi dengan layanan Google lainnya**

Para pengguna layanan Google lainnya akan merasakan kemudahan dalam memanagement file dari Google Drive. Karena Google Drive secara otomatis terintegrasi dengan layanan google lainnya.

- **Fasilitas pencarian**

Google Drive memberikan layanan pencarian yang lebih baik dan lebih cepat untuk para penggunanya dengan menggunakan kata kunci tertentu. Google Drive juga dapat mengenali gambar atau teks dari dokumen hasil scan.

- **Menampilkan berbagai file**

Lebih dari 30 type file yang dapat dibuka dan ditampilkan oleh Google Drive, termasuk file video, file image, dan lain-lain tanpa mengharuskan pengguna untuk mengunduh dan menginstal software yang sesuai dengan tipe atau ekstensi file tersebut.

- **Menjalankan aplikasi**

Google Drive juga mempunyai kemampuan untuk membuat, menjalankan dan membagi file aplikasi favorit yang dimiliki oleh pengguna.

Network Function Virtualization (NFV)

NFV awalnya terbentuk karena banyak provider yang mencari cara tercepat atau mempercepat proses deploy layanan jaringan terbaru untuk membantu meningkatkan pendapatan dan mensuport laju pertumbuhan perusahaan provider tersebut. Kendala yang terjadi akibat sistem yang berbasis hardware menuntun mereka dalam menerapkan sistem virtual berupa standard IT virtualization technologies ke jaringan mereka.

NFV menawarkan cara baru dalam menDesain, menDeploy, dan memanage suatu jaringan atau network service. NFV membagi fungsi-fungsi networking seperti NAT(Network Address Translation), firewalling, deteksi ganguan(intrusion detection), DNS, dan Caching yang berwujud fisik dapat dijalankan dalam bentuk virtual sehingga dapat dijalankan dalam software.

NFV didesain untuk menggabungkan dan mengirim komponen – komponen networking yang dibutuhkan untuk membantu virtualisasi penuh dalam infrastruktur jaringan(Fully virtualized infrastructure).

Jenis – jenis virtualisasi infrastruktur jaringan :

- Virtual Servers
- Storage
- Network
- Dll

NFV memanfaatkan teknologi Standard IT Virtualization seperti high-volume service, catalyst(Switch) dan hardware storage menjadi bentuk fungsi jaringan berbentuk virtual. NFV dapat digunakan di semua data plane procesing atau control plane function pada infrastruktur jaringan berkabel maupun nirkabel (wireless).

Keuntungan NFV :

- Reduce CapEx : mengurangi keperluan untuk membeli hardware yang terlalu banyak sehingga menghilangkan pemborosan yang berlebih
- Reduce OpEx : mengurangi kebutuhan ruang, tenaga, peralatan pendingin dan menyederhanakan peluncuran dan pengelolaan layanan jaringan.
- Accelerate Time-to-Market : mengurangi waktu deploy network service terbaru untuk mendukung bussiness requirement, memanfaatkan peluang pasar baru dan meningkatkan laba untuk balik modal serta dapat mengurangi resiko terkait peluncuran layanan baru dan memudahkan penyedia layanan dalam uji coba dan mengembangkan layanan tersebut untuk menentukan apa yang paling sesuai dengan kebutuhan pelanggan.
- Deliver Agility and Flexibility : mempercepat atau menurunkan skala layanan untuk mengatasi tuntutan perubahan. Mendukung inovasi dengan memungkinkan layanan yang dikirimkan melalui software pada semua jenis hardware server.

Lebih baik mana ? NFV atau SDN ?

SDN dan NFV lebih baik bersama/digabungkan, karena saling menguntungkan dan tidak bergantung pada satu sama lain. Tetapi pada realitanya SDN membuat NFV dan NV lebih menarik dan luas serta visa-versa. SDN berkontribusi dalam network automation yang memungkinkan policy-based decision ke orchestrate menuju lalu lintas jaringan/ network traffic. Sementara NFV berfokus pada layanan. Dan NV menjamin network capabilities align dengan lingkungan virtual mereka.

Perbedaan NFV dan SDN

Category	**SDN**	**NFV**
Reason for Being	Separation of control and data, centralization of control and programmability of network	Relocation of network functions from dedicated appliances to generic servers
Target Location	Campus, data center / cloud	Service provider network
Target Devices	Commodity servers and switches	Commodity servers and switches
Initial Applications	Cloud orchestration and networking	Routers, firewalls, gateways, CDN, WAN accelerators, SLA assurance
New Protocols	OpenFlow	None yet
Formalization	Open Networking Forum (ONF)	ETSI NFV Working Group

CLOUD SECURITY

Cloud computing security adalah keamanan cloud yang mengacu pada serangkaian keamanan teknologi dan kontrol untuk melindungi data, aplikasi dan infrastruktur dalam diagram cloud computing. Cloud security adalah sub-domain dari keamanan komputer, keamanan jaringan, dan lebih luas lagi, keamanan informasi. Arsitektur cloud security hanya efektif jika implementasi defensif yang ada bekerja dengan efesien dan efektif . Arsitektur cloud computing yang efisien harus mengenali masalah yang akan timbul dengan manajemen keamanan. Manajemen keamanan menangani masalah ini dengan kontrol keamanan. Kontrol ini dilakukan untuk melindungi setiap kelemahan dalam sistem dan mengurangi efek serangan. Control keamanan adalah: '... pengamanan atau penanggulangan untuk menghindari, melcloud atau meminimalkan risiko keamanan.'

Jenis-jenis control :

- Deterrent controls

Kontrol ini dimaksudkan untuk mengurangi serangan terhadap sistem cloud. Sama seperti tanda peringatan di pagar atau properti, kontrol pencegah biasanya mengurangi tingkat ancaman dengan menginformasikan penyerang potensial bahwa akan ada konsekuensi buruk bagi mereka jika mereka melanjutkan. (Beberapa menganggap mereka sebagai subset dari kontrol preventif.)

- Preventive controls

Kontrol pencegahan memperkuat sistem terhadap insiden, umumnya dengan mengurangi jika tidak benar-benar menghilangkan kerentanan. Otentikasi kuat pengguna cloud, misalnya, membuat kecil kemungkinan pengguna yang tidak sah dapat mengakses sistem cloud, dan kemungkinan besar pengguna cloud diidentifikasi secara positif.

- Detective controls

Kontrol detektif dimaksudkan untuk mendeteksi dan bereaksi secara tepat terhadap kejadian yang terjadi. Jika terjadi serangan, kontrol detektif akan memberi sinyal kontrol pencegahan atau koreksi untuk mengatasi masalah ini. Pemantauan keamanan sistem dan jaringan, termasuk pengaturan deteksi dan pencegahan intrusi, biasanya digunakan untuk mendeteksi serangan terhadap sistem cloud dan infrastruktur komunikasi pendukung.

- Corrective controls

Kontrol korektif mengurangi konsekuensi insiden, biasanya dengan membatasi kerusakan. Mereka mulai berlaku selama atau setelah sebuah kejadian. Memulihkan backup sistem untuk membangun kembali sistem yang dikompromikan adalah contoh kontrol korektif.

SECURITY DAN PRIVASI

Identity management

Penyedia cloud mengintegrasikan sistem manajemen identitas pelanggan ke dalam infrastruktur mereka sendiri, menggunakan teknologi federasi atau SSO, atau sistem identifikasi berbasis biometrik, atau menyediakan sistem pengelolaan identitas diri mereka sendiri. CloudID, misalnya, menyediakan identifikasi biometrik berbasis cloud dan cross-enterprise yang melindungi privasi. Ini menghubungkan informasi rahasia pengguna dengan biometrik mereka dan menyimpannya dalam mode terenkripsi. Dengan menggunakan teknik enkripsi yang mudah dicari, identifikasi biometrik dilakukan di domain terenkripsi untuk memastikan bahwa penyedia cloud atau penyerang potensial tidak mendapatkan akses ke data sensitif atau bahkan isi dari kueri individual.

- physical security

Penyedia layanan cloud secara fisik mengamankan perangkat keras TI (server, router, kabel dll.) Terhadap akses yang tidak sah, gangguan, pencurian, kebakaran, banjir dll dan memastikan bahwa persediaan penting (seperti listrik) cukup kuat untuk meminimalkan kemungkinan gangguan. Hal ini biasanya dicapai dengan melayani aplikasi cloud dari pusat data 'kelas dunia' (yaitu pusat data, klasifikasi, perawatan, konstruksi, pemantauan, dan pemeliharaan yang dirancang secara khusus, dirancang, dibangun, dikelola, dipantau dan dipelihara).

- personal security

Berbagai masalah keamanan informasi yang berkaitan dengan TI dan profesional lainnya yang terkait dengan layanan cloud biasanya ditangani melalui kegiatan pra, paragraf dan pasca kerja seperti perekrutan potensial perekrutan, program kesadaran keamanan dan pelatihan, proaktif.

- privasi

Penyedia memastikan bahwa semua data penting (nomor kartu kredit, misalnya) ditutupi atau dienkripsi dan hanya pengguna yang berwenang yang memiliki akses ke data secara keseluruhan. Selain itu, identitas dan kredensial digital harus dilindungi seolah-olah data yang dikumpulkan atau dikumpulkan oleh penyedia layanan tentang aktivitas pelanggan di cloud.

Data security

Sejumlah ancaman keamanan dikaitkan dengan layanan data cloud: tidak hanya ancaman keamanan tradisional, seperti penyadapan jaringan, invasi ilegal, dan serangan penolakan layanan, namun juga ancaman komputasi cloud yang spesifik, seperti serangan saluran samping, kerentanan virtualisasi, dan penyalahgunaan Layanan cloud Persyaratan keamanan berikut membatasi ancaman.

- Confidentiality

Kerahasiaan data adalah properti yang isinya tidak tersedia atau diungkapkan kepada pengguna ilegal. Data outsource disimpan di cloud dan di luar kontrol. Hanya pengguna yang berwenang yang dapat mengakses data sensitif sementara yang lain,
termasuk CSP, tidak boleh mendapatkan informasi apapun dari data tersebut. Sementara itu, pemilik data berharap dapat memanfaatkan sepenuhnya layanan data cloud, misalnya, pencarian data, penghitungan data, dan berbagi data, tanpa kebocoran isi data ke CSP atau musuh lainnya.

- Access controllability

Access controllability berarti pemilik data dapat melakukan pembatasan selektif terhadap akses ke data yang dioutsourcing ke cloud. Pengguna hukum dapat diberi wewenang oleh pemiliknya untuk mengakses data, sementara yang lain tidak dapat mengaksesnya tanpa izin. Selanjutnya, diinginkan untuk menerapkan kontrol akses berbutir halus ke data yang dioutsource, yaitu, pengguna yang berbeda harus diberikan hak akses yang berbeda berkenaan dengan potongan data yang berbeda. Otorisasi akses harus dikontrol hanya oleh pemilik di lingkungan cloud yang tidak tepercaya.

- Integrity

Integritas data menuntut pemeliharaan dan memastikan keakuratan dan kelengkapan data. Seorang pemilik data selalu mengharapkan agar datanya di cloud dapat disimpan dengan benar dan dapat dipercaya. Ini berarti bahwa data tidak boleh dirusak secara ilegal, dimodifikasi secara tidak benar, sengaja dihapus, atau dibuat dengan jahat. Jika ada operasi yang tidak diinginkan yang merusak atau menghapus data, pemilik harus dapat mendeteksi korup. Selanjutnya, bila sebagian data yang dioutsourcing rusak atau hilang, data tersebut masih dapat diambil oleh pengguna data.