INTERKONEKSI SMK TKJ SE-DEPOK with VPN L2TP IPSEC & DOCKER CONTAINER

MUM ID, 15 Oktober 2020

PRESENTED BY ALI IMRAN

About Me

Ali Imran

- Studies : STT Terpadu Nurul Fikri
- Profession :
  - Computer Teacher
    - SMK Harapan Bangsa
    - SMK Al Muhajirin
  - Freelancer Engineer
- Certification in MikroTik :
  - MTCNA, MTCRE, MTCINE, MTCWE, MTCUME, MTCIPv6E, MTCTCE, MTCSE
  - ACTR #1080
  - Certified MikroTik Consultant
- More Info :
  - https://www.linkedin.com/in/alinux1999/

ITCLUB
Networking & Infrastucture
Sekolah Tinggi Terpadu Nurul Fikri

NETS is a student organization at STT Terpadu Nurul Fikri to discuss and study computer network science, especially MikroTik, and routinely hold MTCNA certification classes.

www.aliimran.id
fb.com/alinux1999
alinux1999@gmail.com
@alinux.id

SMK HARAPAN BANGSA

Presentation Background

- SMK TKJ Depok mean is Computer Network Vocational School in Depok City, totaled 41 schools. we want to build a network that can connect all schools for student knowledge and used for sharing between schools.
- Benefits :
  - sharing connection
  - sharing data
  - knowledge for teachers and students
- Problem :
  - expensive cost, because we have to buy a lot of tools such as cables, etc.
  - takes a long time
  - not easy to build
- Solution is interconnection with VPN L2TP IPSec using Docker Container
  - easy to build
  - does not take a long time
  - not expensive cost

Presentation materials

- Introduction MGMP TKJ Depok
- L2TP
- IPSec
- Routing OSPF
- Container n Docker
- Summary
- References

Depok City Map

ABOUT MGMP TKJ DEPOK

MGMP TKJ Depok is an organization of TKJ teachers from all TKJ schools in Depok City, which was founded in 2017.

The main activity of this organization is to establish friendship and share information or about technology with their respective schools.

https://s.id/peta-tkj-depok

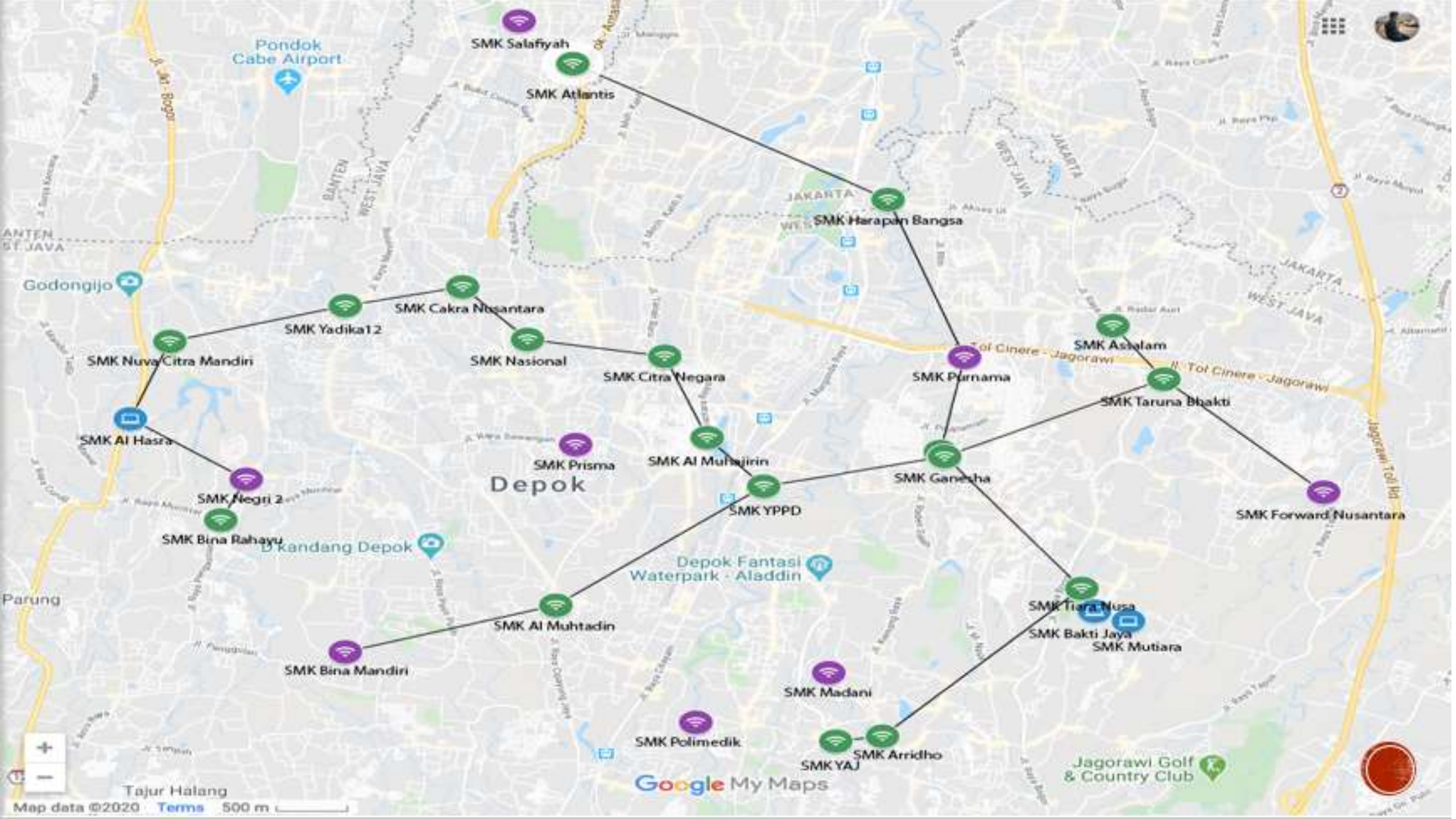

SMK Salafiyah
SMK Atlantis
SMK Harapan Bangsa
SMK Cakra Nusantara
SMK Yadika12
SMK Nuva Citra Mandiri
SMK Nasional
SMK Citra Negara
SMK Al Hasra
SMK Prisma
SMK Al Muhajirin
SMK Purnama
SMK Asalam
SMK Taruna Bhakti
SMK Ganesha
SMK Forward Nusantara
SMK Negri 2
SMK Bina Rahayu
SMK YPPD
SMK Al Muhtadin
SMK Bina Mandiri
SMK Tiara Nusa
SMK Bakti Jaya
SMK Mutiara
SMK Madani
SMK Polimedik
SMK YAJ
SMK Arridho
Pondok Cabe Airport
Godongjio
Depok
D'kandang Depok
Depok Fantasi Waterpark · Aladdin
Parung
Tajur Halang
Jagorawi Golf & Country Club
Tol Cinere - Jagorawi
Jagorawi Tol Rd
JAKARTA
WEST JAVA
BANTEN
Google My Maps
Map data ©2020
Terms
500 m

Photo MGMP TKJ

VIRTUAL PRIVATE NETWORK

- VPN is a secure way to access local area network using internet or public network.
- A **virtual private network** (**VPN**) extends a private network across a public network and enables users to send and receive data across shared or public networks as if their computing devices were directly connected to the private network.

- Benefits of VPNs :
  - Cost savings
  - Scalability
  - Security

TYPE OF VPN

- Remote Access
  - connecting an individual computer to a network.
- Site to Site
  - connecting two networks together.
- Hub and Spoke
  - connecting many network to vpn concentrator.

L2TP

- L2TP stands for Layer 2 Tunnelling Protocol. L2TP was first proposed in 1999 as an upgrade to both L2F (Layer 2 Forwarding Protocol) and PPTP (Point-to-Point Tunnelling Protocol)
- L2TP uses UDP port 1701.
- L2TP by default use MPPE 128Bit as used in PPTP.

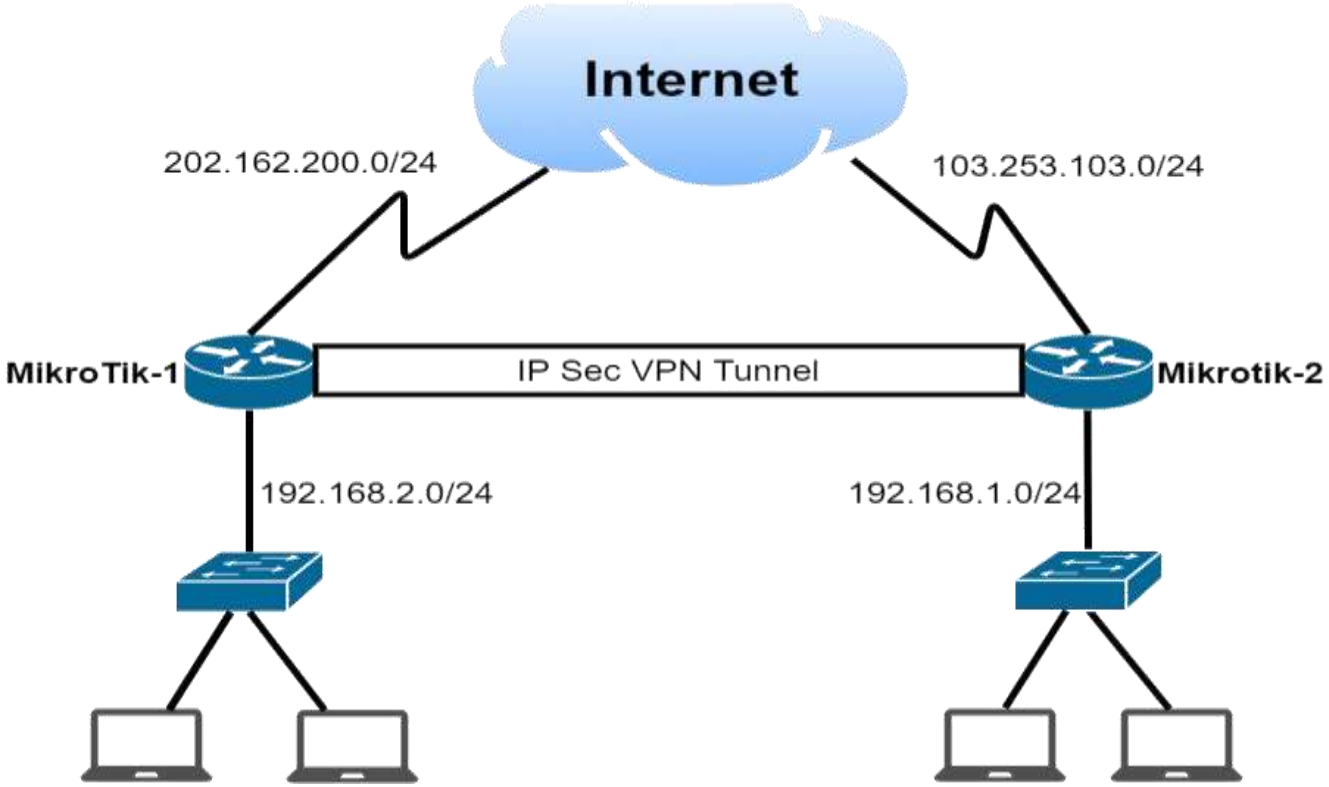
IP SECURITY

- Internet Protocol Security (IPsec) is a set of protocols defined by the Internet Engineering Task Force (IETF) to secure packet exchange over unprotected IPv4 or IPv6 networks such as Internet. Provides Layer 3 security (RFC 2401)

IPsec Combines different components :

- Security associations (SA)
- Authentication headers(AH)
- Encapsulating security payload (ESP)
- Internet Key Exchange (IKE)

IP SECURITY


Internet
202.162.200.0/24
103.253.103.0/24
MikroTik-1
IP Sec VPN Tunnel
Mikrotik-2
192.168.2.0/24
192.168.1.0/24

IPSEC BENEFITS

Confidentiality

- By encrypting data

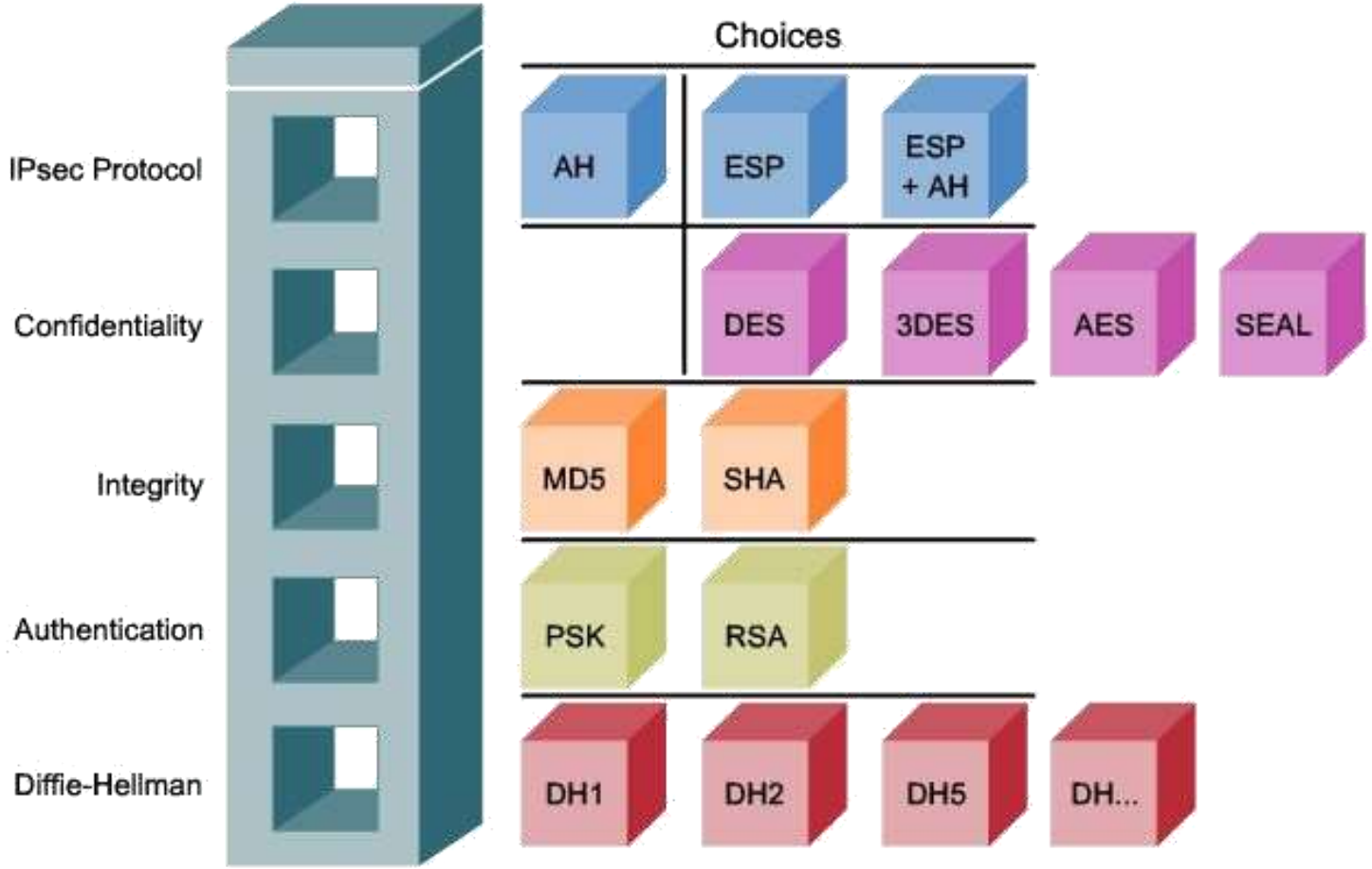
Integrity

- Routers at each end of a tunnel calculates the checksum or hash value of the data

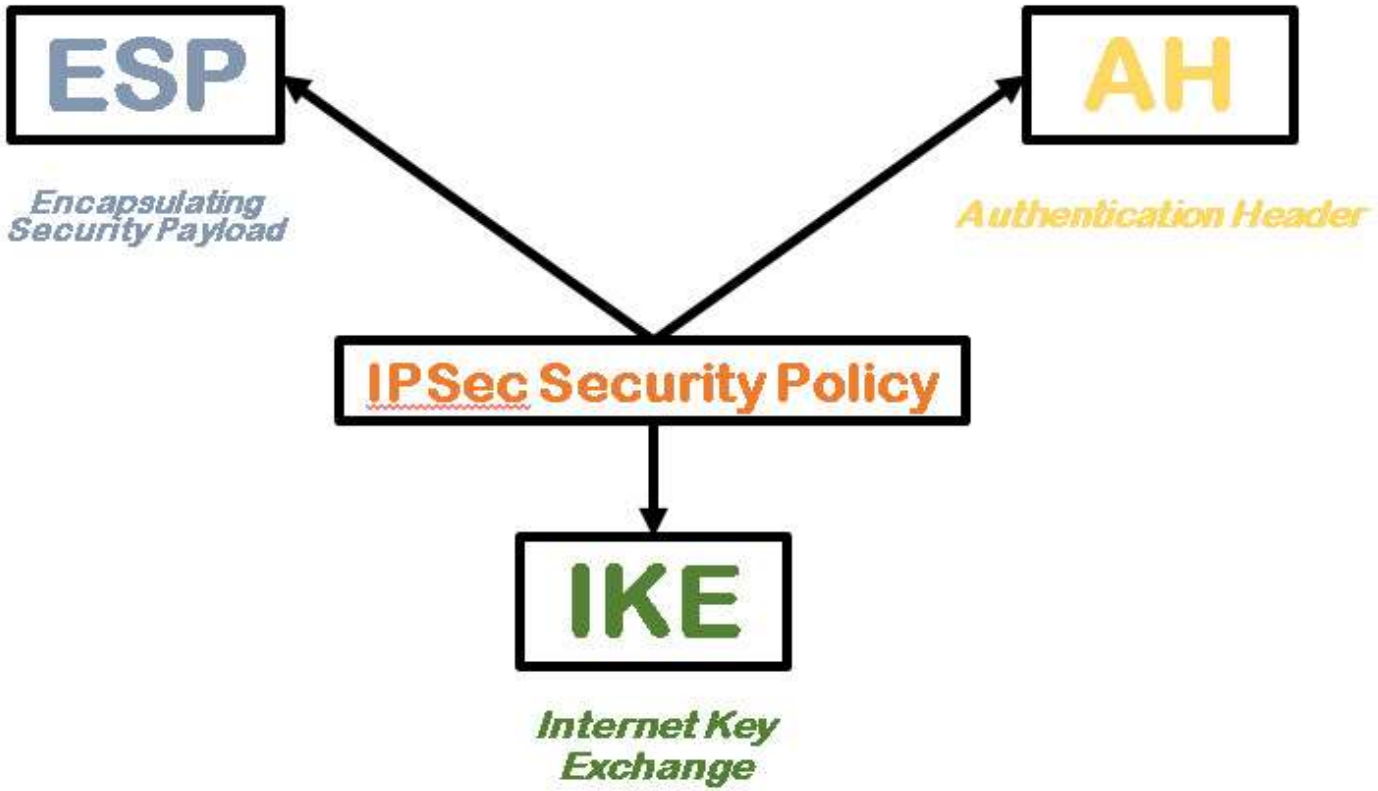
Authentication

- Signatures and certificates
- All these while still maintaining the ability to route through existing IP Networks

IPSEC FRAMEWORK



IPSEC ARCHITECTURE



Encapsulating Security Payload

- Encapsulating Security Payload (ESP) uses shared key encryption to provide data privacy. ESP also supports its own authentication scheme like that used in AH, or can be used in conjunction with AH.
- ESP packages its fields in a very different way than AH. Instead of having just a header, it divides its fields into three components:
  - ESP Header: Comes before the encrypted data and its placement depends on whether ESP is used in transport mode or tunnel mode.
  - ESP Trailer :This section is placed after the encrypted data. It contains padding that is used to align the encrypted data.
  - ESP Auth Data : This field contains an Integrity Check Value (ICV), computed in a manner similar to how the AH protocol works, for when ESP's optional authentication feature is used.

ENCAPSULATING SECURITY PAYLOAD

- Uses IP protocol 50
- Provides all that is offered by AH, plus data confidentiality
    - It uses symmetric key encryption
- Must encrypt and/or authenticate in each packet
    - Encryption occurs before authentication
- Authentication is applied to data in the IPsec header as well as the data contained as payload

Authentication : SHA1, MD5
Encryption : DES, 3DES, AES, Blowfish, Twofish, Camellia

AUTHENTICATION HEADER

AH is a protocol that provides authentication of either all or part of the contents of a datagram through the addition of a header that is calculated based on the values in the datagram.

What parts of the datagram are used for the calculation, and the placement of the header, depends whether tunnel or transport mode is used.

- Provides source authentication and data integrity
- Authentication is applied to the entire packet, with the mutable fields in the IP header zeroed out
- Operates on top of IP using protocol 51
- In IPv4, AH protects the payload and all header fields except mutable fields and IP options (such as IPsec option)

MikroTik RouterOS supports the following authentication algorithms for AH:

- SHA1 • MD5

IKE (INTERNET KEY EXCHANGE)

The Internet Key Exchange (IKE) is a protocol that provides authenticated keying material for Internet Security Association and Key Management Protocol (ISAKMP) framework. There are other key exchange schemes that work with ISAKMP, but IKE is the most widely used one. Together they provide means for authentication of hosts and automatic management of security associations (SA).

- Typically used for establishing IPSec sessions
- A key exchange mechanism
- Three authentication methods (pre-shared, public key encryption, and public key signature)
- Uses UDP port 500

IKE MODE :

Main Mode, Aggressive mode, Quick Mode.

IKE (TWO PHASE)

- Phase 1:

The peers agree upon algorithms they will use in the following IKE messages and authenticate. The keying material used to derive keys for all SAs and to protect following ISAKMP exchanges between hosts is generated also

- Phase 2:

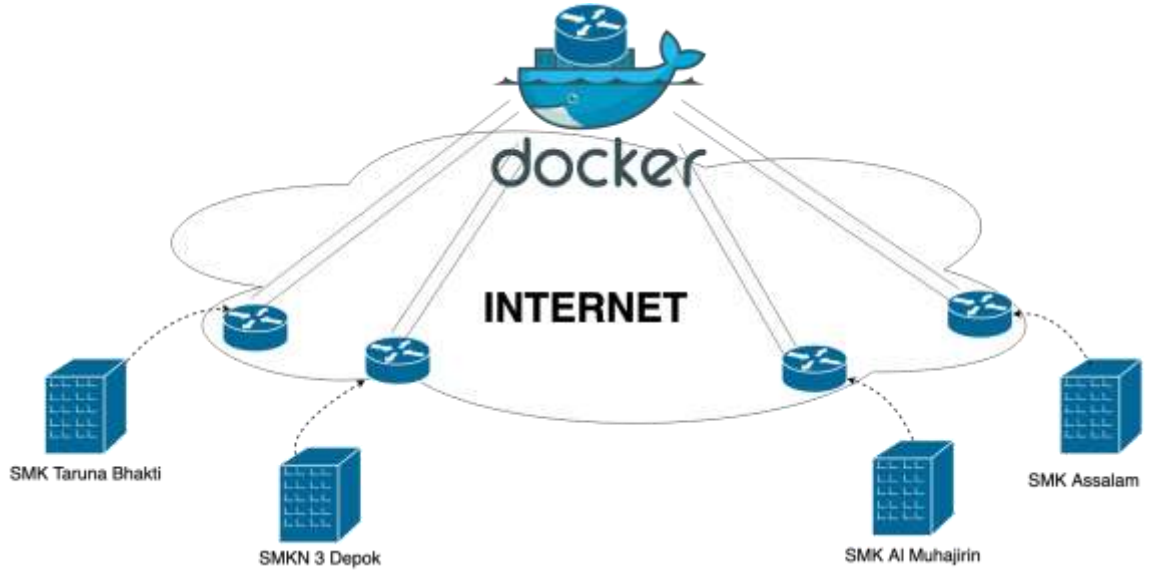
The peers establish one or more SAs that will be used by IPsec to encrypt data. All SAs established by IKE daemon will have lifetime values (either limiting time, after which SA will become invalid, or amount of data that can be encrypted by this SA, or both)

Phase 1 IKE	Phase 2 IPsec
Auth Method	Ipsec Protocol
DH Group	Mode (Tun or Tap)
Encryption algorithm	Auth Method
Exchange mode	PFS (DH group)
Hash algorithm	Lifetime
NAT-T	
DPD and Lifetime	

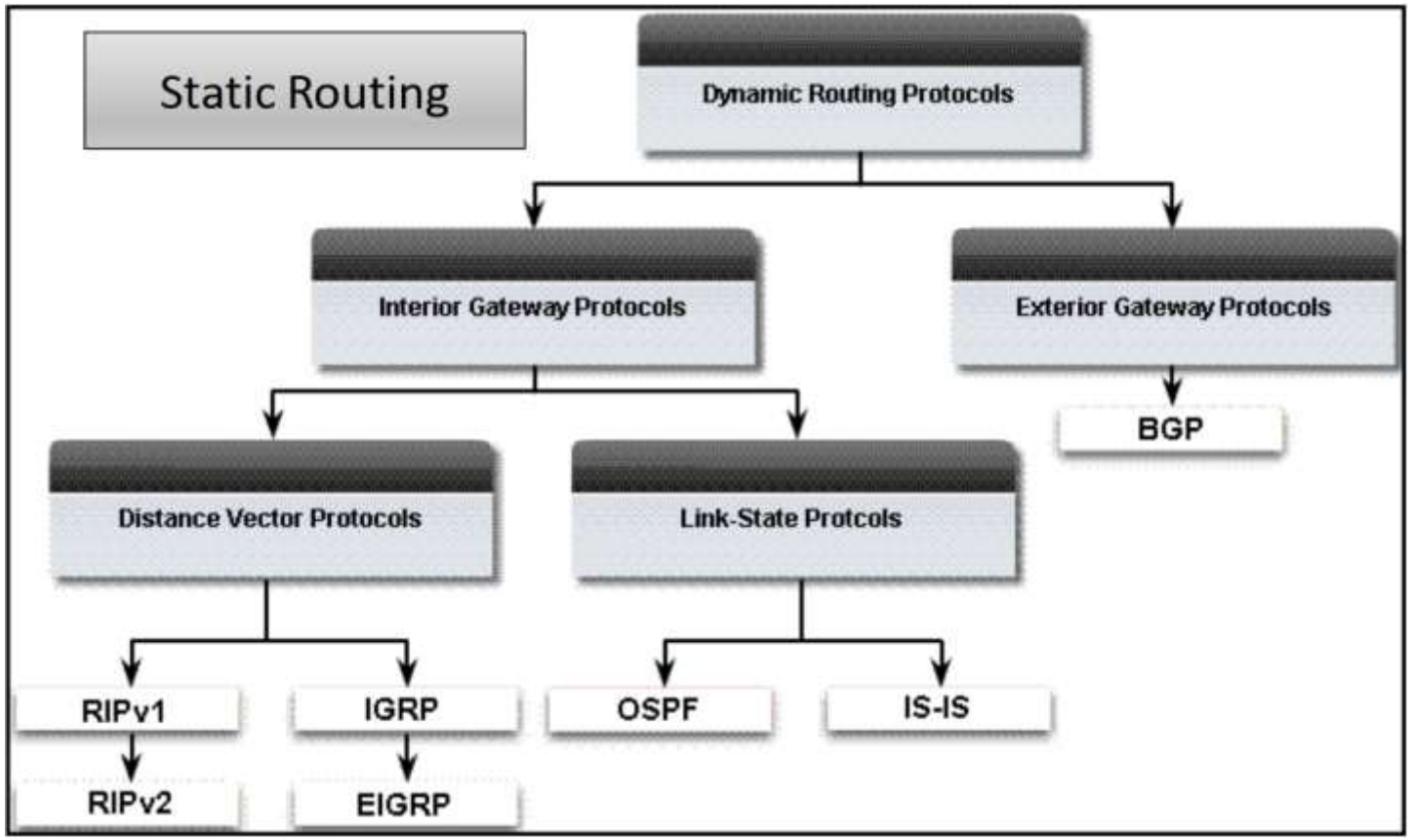
ROUTING

Routing is the process of selecting a path for traffic in a network or between or across multiple networks.

Routing is used for forwarding packet with a router.



ROUTING CLASIFICATION



OSPF (OPEN SHORTS PATH FAST)

- Open Shortest Path First (OSPF) is an automatic routing protocol (Dynamic Routing) capable of maintaining, managing and distributing routing information between networks dynamically following any network changes.
- OSPF is included in the IGP (Interior Gateway Protocol) category which has Link-state capabilities and Dijkstra's Algorithm which is much more efficient than other IGP protocols.
- OSPF is used to manage routing information and distribution within an AS.
- OSPF uses protocol 89

CONTAINER

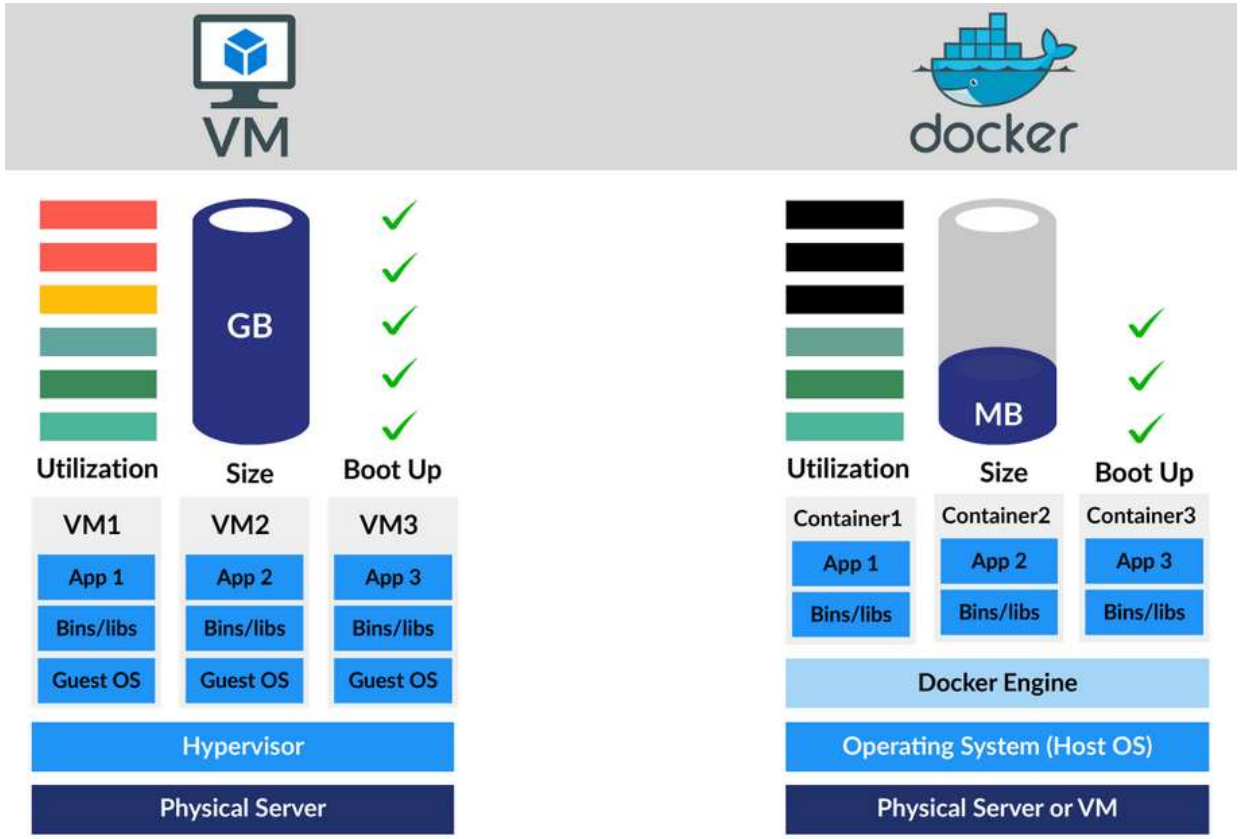
- container is an OS virtualization that can package an application with its dependencies and environment.
- Each of these containers has an isolated process so it doesn't interfere with the host OS or other containers.

- Benefits of Container :
  - Flexible and scalable
  - Reducing the resources needed in IT Management
  - Fast (deployment, migration, restarts)

DOCKER

- Docker is an open platform for developing, shipping, and running applications.
- Docker allows you to package an application with all of its dependencies into a standardized unit for software development.
- Almost similar to a Virtual Machine (VM) but lighter. Because Docker does not carry the entire operating system, only shares the system (system shared) with the host.

DOCKER VS VM


VM
GB
Utilization
Size
Boot Up
VM1
VM2
VM3
App 1
App 2
App 3
Bins/libs
Bins/libs
Bins/libs
Guest OS
Guest OS
Guest OS
Hypervisor
Physical Server
docker
MB
Utilization
Size
Boot Up
Container1
Container2
Container3
App 1
App 2
App 3
Bins/libs
Bins/libs
Bins/libs
Docker Engine
Operating System (Host OS)
Physical Server or VM

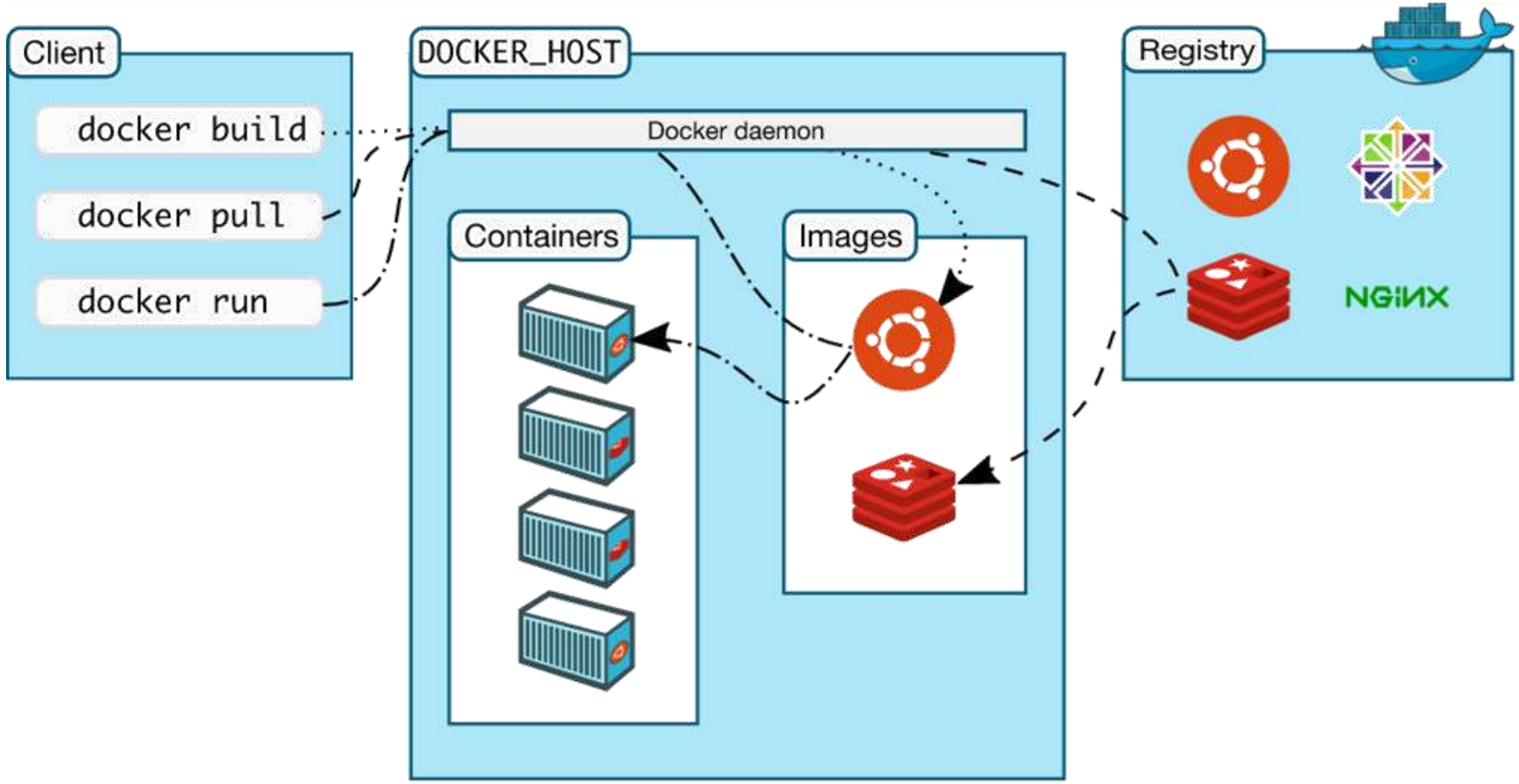
DOCKER BENEFITS

- Fast (deployment, migration, restarts)
- Secure
- Lightweight (save disk & CPU)
- Open Source
- Portable software
- Multi Cloud platform

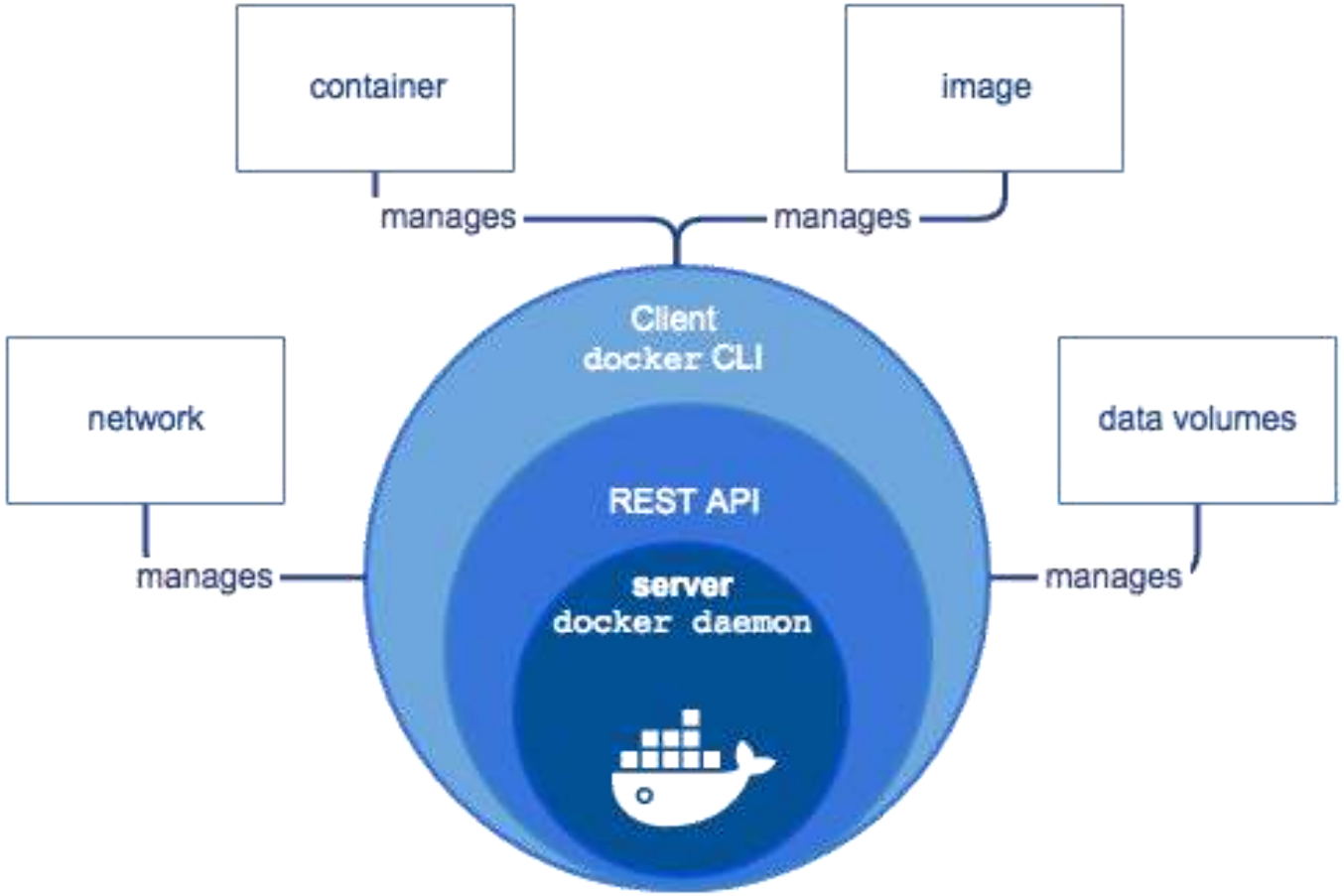
DOCKER SUPPORT (MULTIPLE PLATFORM)

https://docs.docker.com/get-docker/

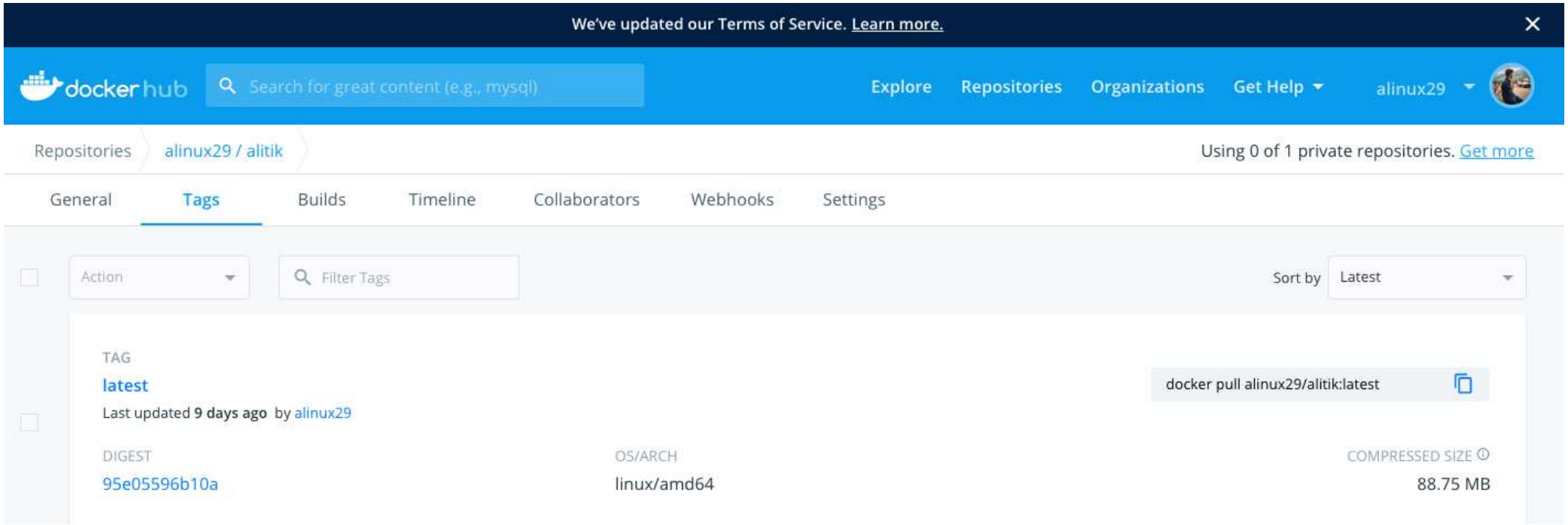
DOCKER ARCHITECTURE



DOCKER COMPONENT



DOCKER HUB



Command to pull image MikroTik = Docker pull alinux29/alitik

DOCKER COMMAND

- docker push alinux29/alitik
- docker run -itd --name=MikroTik --cap-add=NET_ADMIN --device=/dev/net/tun alinux29/alitik
- docker ps
- docker inspect MikroTik
- ping 172.17.0.2
- ssh admin@172.17.0.2

REFERENCES

- Wiki mikrotik l2tp https://wiki.mikrotik.com/wiki/Manual:Interface/L2TP
- Wiki mikrotik ipsec https://wiki.mikrotik.com/wiki/Manual:IP/IPsec
- Wiki mikrotik ospf https://wiki.mikrotik.com/wiki/Manual:Routing/OSPF
- Docker Documentation https://docs.docker.com
- RouterOS Docker https://github.com/EvilFreelancer/docker-routeros

ANY QUESTIONS

alinux.id

www.aliimran.id

THANK YOU!

 www.aliimran.id

 fb.com/alinux1999

 alinux1999@gmail.com

 @alinux.id