Sécurité dans les environnements infonuagiques

Module 3: Gestion des Configurations (Part 1)

Armstrong Foundjem

Polytechnique Montréal

Automne 2023

Plan

1. Network models
2. Network security concepts
3. VPC & EC2 security (in Part 2)

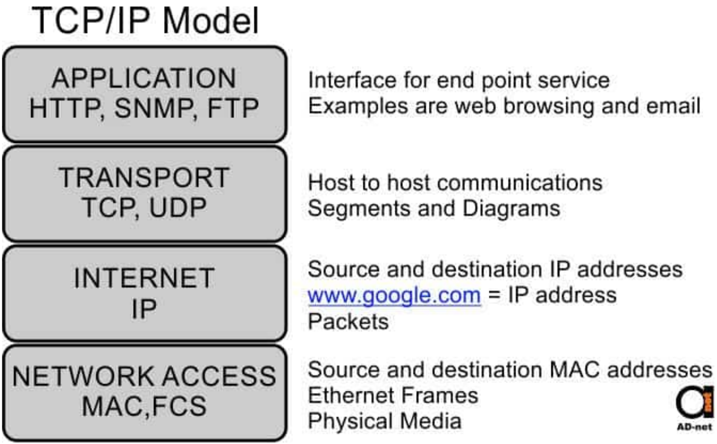
1 Network models

2 Network security concepts

TCP/IP Model

- designed and developed by the US Department of Defense (DoD)
- allows host-to-host communication through network
- has 4 layers: network access, Internet, transport, and application.
- **Advantages**: More reliable, application layer combines session and presentation layer
- **Disadvantages**: does not provide assurance delivery of packets, protocols cannot be replaced easily

TCP/IP Model



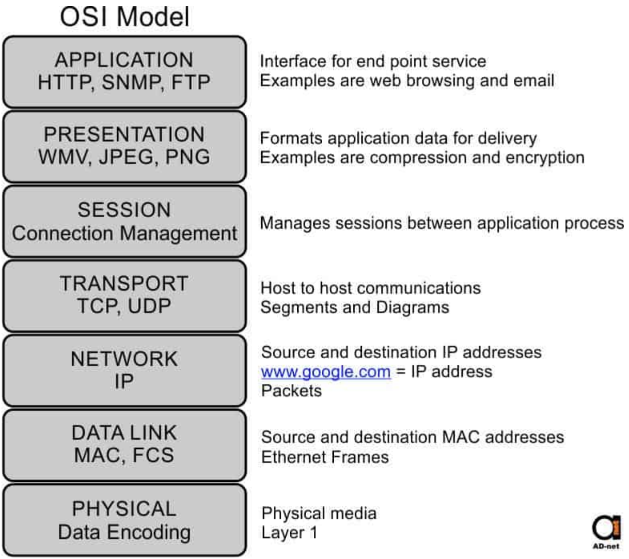
TCP/IP Model

APPLICATION HTTP, SNMP, FTP	Interface for end point service Examples are web browsing and email
TRANSPORT TCP, UDP	Host to host communications Segments and Diagrams
INTERNET IP	Source and destination IP addresses www.google.com = IP address Packets
NETWORK ACCESS MAC,FCS	Source and destination MAC addresses Ethernet Frames Physical Media

OSI Model

- allows host-to-host communication through network
- has 7 layers: physical, data link, network, transport, session, presentation, and application
- **Advantages**: provides assurance delivery of packets, protocols can be replaced easily,
- **Disadvantages**: Less reliable than TCP/IP, session and presentation layer are separated

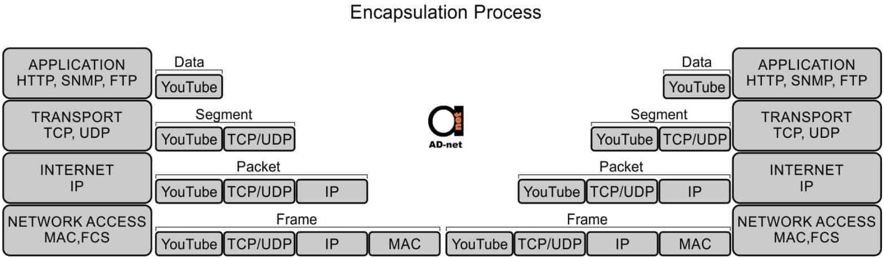
OSI Model



OSI Model

APPLICATION HTTP, SNMP, FTP	Interface for end point service Examples are web browsing and email
PRESENTATION WMV, JPEG, PNG	Formats application data for delivery Examples are compression and encryption
SESSION Connection Management	Manages sessions between application process
TRANSPORT TCP, UDP	Host to host communications Segments and Diagrams
NETWORK IP	Source and destination IP addresses www.google.com = IP address Packets
DATA LINK MAC, FCS	Source and destination MAC addresses Ethernet Frames
PHYSICAL Data Encoding	Physical media Layer 1

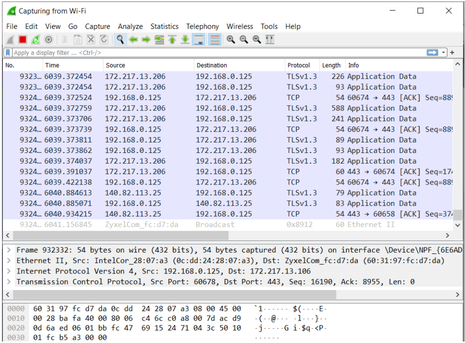
Network Encapsulation



- Encapsulation promotes maintenance
- Code changes are modular i.e. it can be made independently
- Better usability

Network Encapsulation

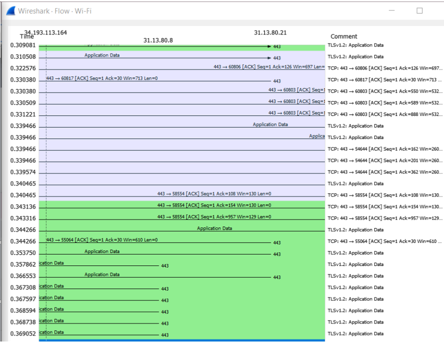
- **What is the 3-way TCP handshake ?**
- On Wireshark, open **Statistics** > **Flow Graph**


Capturing from Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
9323…	6039.372454	172.217.13.206	192.168.0.125	TLSv1.3	226	Application Data
9323…	6039.372454	172.217.13.206	192.168.0.125	TLSv1.3	93	Application Data
9324…	6039.372524	192.168.0.125	172.217.13.206	TCP	54	60674 → 443 [ACK] Seq=88
9324…	6039.372759	172.217.13.206	192.168.0.125	TLSv1.3	588	Application Data
9324…	6039.373706	172.217.13.206	192.168.0.125	TLSv1.3	241	Application Data
9324…	6039.373739	192.168.0.125	172.217.13.206	TCP	54	60674 → 443 [ACK] Seq=88
9324…	6039.373811	192.168.0.125	172.217.13.206	TLSv1.3	89	Application Data
9324…	6039.373862	192.168.0.125	172.217.13.206	TLSv1.3	93	Application Data
9324…	6039.374037	172.217.13.206	192.168.0.125	TLSv1.3	182	Application Data
9324…	6039.391037	172.217.13.206	192.168.0.125	TCP	60	443 → 60674 [ACK] Seq=17
9324…	6039.422138	192.168.0.125	172.217.13.206	TCP	54	60674 → 443 [ACK] Seq=88
9324…	6040.884613	140.82.113.25	192.168.0.125	TLSv1.3	79	Application Data
9324…	6040.885071	192.168.0.125	140.82.113.25	TLSv1.3	83	Application Data
9324…	6040.934215	140.82.113.25	192.168.0.125	TCP	54	443 → 60658 [ACK] Seq=37
9324…	6041.156845	ZyxelCom_fc:d7:da	Broadcast	0x8912	60	Ethernet II

```
> Frame 932332: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface \Device\NPF_{6E6AD
> Ethernet II, Src: IntelCor_28:07:a3 (0c:dd:24:28:07:a3), Dst: ZyxelCom_fc:d7:da (60:31:97:fc:d7:da)
> Internet Protocol Version 4, Src: 192.168.0.125, Dst: 172.217.13.106
> Transmission Control Protocol, Src Port: 60678, Dst Port: 443, Seq: 16190, Ack: 8955, Len: 0
```

```
0000  60 31 97 fc d7 da 0c dd  24 28 07 a3 08 00 45 00   `1······ $(····E·
0010  00 28 ba fa 40 00 80 06  c4 6c c0 a8 00 7d ac d9   ·(··@··· ·l···}··
0020  0d 6a ed 06 01 bb fc 47  69 15 24 71 04 3c 50 10   ·j·····G i·$q·<P·
0030  01 fc b5 a3 00 00                                  ······
```


Wireshark · Flow · Wi-Fi
34.193.113.164
31.13.80.8
31.13.80.21
Application Data
443 → 60806 [ACK] Seq=1 Ack=126 Win=697 Len=
443 → 60817 [ACK] Seq=1 Ack=30 Win=713 Len=0
443 → 60803 [ACK] Seq=1
443 → 58554 [ACK] Seq=1 Ack=108 Win=130 Len=0
443 → 58554 [ACK] Seq=1 Ack=154 Win=130 Len=0
443 → 58554 [ACK] Seq=1 Ack=957 Win=129 Len=0
443 → 55064 [ACK] Seq=1 Ack=30 Win=610 Len=0
443

Time	Comment
0.309081	TLSv1.2: Application Data
0.310508	TLSv1.2: Application Data
0.322576	TCP: 443 → 60806 [ACK] Seq=1 Ack=126 Win=697…
0.330380	TCP: 443 → 60817 [ACK] Seq=1 Ack=30 Win=713 …
0.330380	TCP: 443 → 60803 [ACK] Seq=1 Ack=550 Win=532…
0.330509	TCP: 443 → 60803 [ACK] Seq=1 Ack=589 Win=532…
0.331221	TCP: 443 → 60803 [ACK] Seq=1 Ack=888 Win=532…
0.339466	TLSv1.2: Application Data
0.339466	TLSv1.2: Application Data
0.339466	TCP: 443 → 54644 [ACK] Seq=1 Ack=162 Win=260…
0.339466	TCP: 443 → 54644 [ACK] Seq=1 Ack=201 Win=260…
0.339574	TCP: 443 → 54644 [ACK] Seq=1 Ack=362 Win=260…
0.340465	TLSv1.2: Application Data
0.340465	TCP: 443 → 58554 [ACK] Seq=1 Ack=108 Win=130…
0.343136	TCP: 443 → 58554 [ACK] Seq=1 Ack=154 Win=130…
0.343316	TCP: 443 → 58554 [ACK] Seq=1 Ack=957 Win=129…
0.344266	TLSv1.2: Application Data
0.344266	TCP: 443 → 55064 [ACK] Seq=1 Ack=30 Win=610 …
0.353750	TLSv1.2: Application Data
0.357862	TLSv1.2: Application Data
0.366553	TLSv1.2: Application Data
0.367308	TLSv1.2: Application Data
0.367597	TLSv1.2: Application Data
0.368594	TLSv1.2: Application Data
0.368738	TLSv1.2: Application Data
0.369052	TLSv1.2: Application Data

Sondage ☺: https://app.wooclap.com/PGISKC.

wooclap

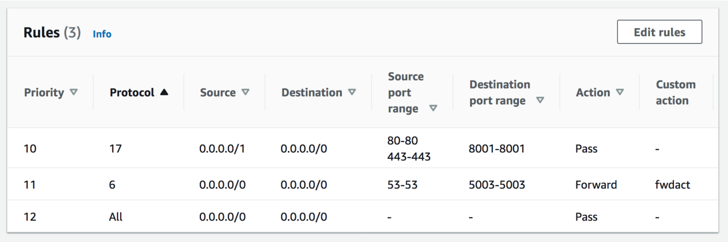
1 Network models

2 Network security concepts

Network Firewall

- It uses a rule table to accept/reject/forward network packets
- The rule table consists of network rules on inbound and and outbound network packets
- For example, the rule

```
pass tls any any -> any any (tls.sni; content:"polymtl.ca"; startswith;
nocase; endswith; msg:"Permit HTTPS access to polymtl.ca"; sid:1000002;
rev:1;)
```

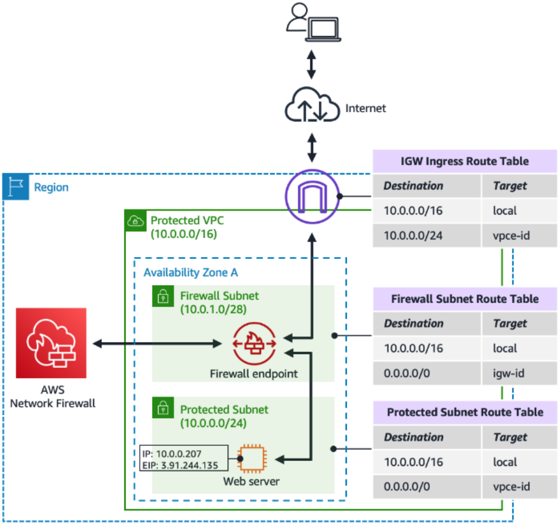


Rules (3) Info

Edit rules

Priority ▽	Protocol ▲	Source ▽	Destination ▽	Source port range ▽	Destination port range ▽	Action ▽	Custom action
10	17	0.0.0.0/1	0.0.0.0/0	80-80 443-443	8001-8001	Pass	-
11	6	0.0.0.0/0	0.0.0.0/0	53-53	5003-5003	Forward	fwdact
12	All	0.0.0.0/0	0.0.0.0/0	-	-	Pass	-

Network Firewall



IGW Ingress Route Table

Destination	*Target*
10.0.0.0/16	local
10.0.0.0/24	vpce-id

Firewall Subnet Route Table

Destination	*Target*
10.0.0.0/16	local
0.0.0.0/0	igw-id

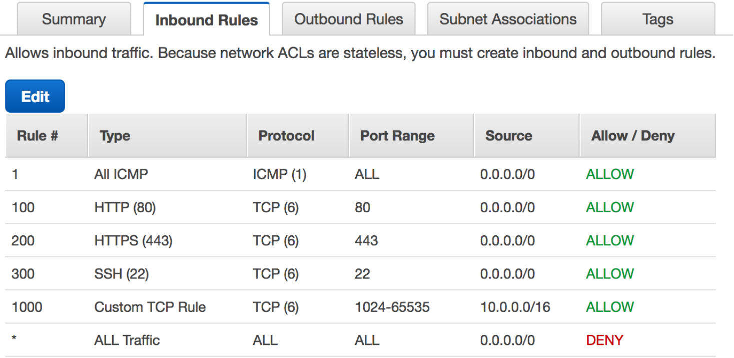
Protected Subnet Route Table

Destination	*Target*
10.0.0.0/16	local
0.0.0.0/0	vpce-id

Credits: Amazon

Network Access Control List

- controls the inbound and outbound traffic at the subnet level
- it uses a rule table to accept/reject/forward traffic on subnets



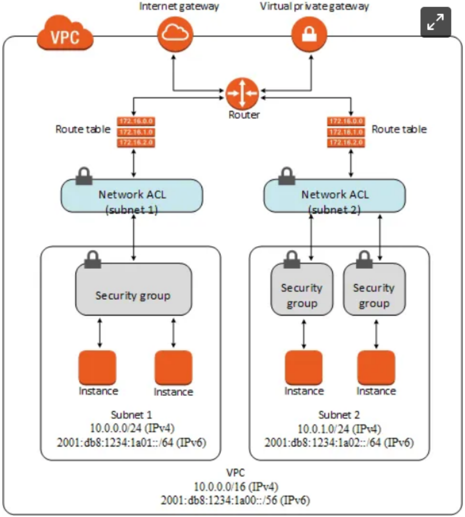
Allows inbound traffic. Because network ACLs are stateless, you must create inbound and outbound rules.

Rule #	Type	Protocol	Port Range	Source	Allow / Deny
1	All ICMP	ICMP (1)	ALL	0.0.0.0/0	ALLOW
100	HTTP (80)	TCP (6)	80	0.0.0.0/0	ALLOW
200	HTTPS (443)	TCP (6)	443	0.0.0.0/0	ALLOW
300	SSH (22)	TCP (6)	22	0.0.0.0/0	ALLOW
1000	Custom TCP Rule	TCP (6)	1024-65535	10.0.0.0/16	ALLOW
*	ALL Traffic	ALL	ALL	0.0.0.0/0	DENY

Security Groups

- allows one to define network access control rules that apply to a group
- All resources and subnets *RS* attached with a security group *S* are controlled by the same rules
- Security group can be attached to an EC2 instance, a subnet, or a virtual private cloud

Security Groups

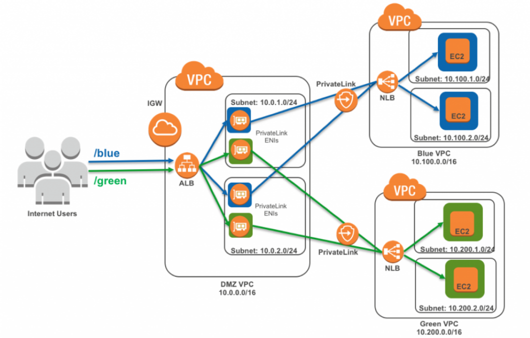


Network Load Balancer

- automatically distributes traffic workloads
- across multiple network nodes such as IP addresses, EC2 instances or containers
- in one or more Availability Zones to increase the fault tolerance
- by selecting targets on network flow information (e.g., protocol, src IP, src port, dest IP, and dest port)
- It uses different algorithms for selection: round-robin, distributed Hashing, consistent Hashing
- **What is the difference between an application load balancer and a network load balancer ?**
- **How Load balancing can help in blue-green deployment ?**

Network Load Balancer

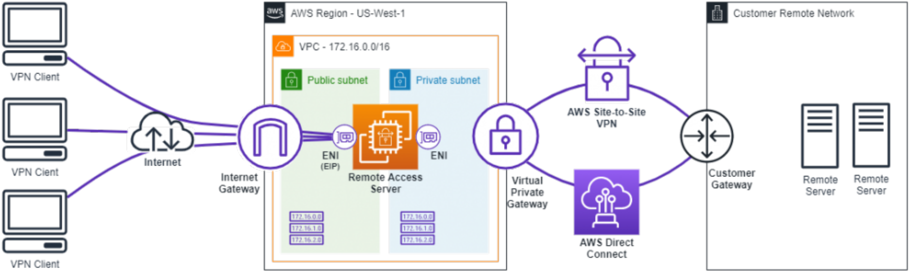
- a blue/green deployment is a near-zero downtime strategy with two identical environments where
  - blue environment is running the current application version
  - green environment is running the new application version
- load balancing distributes old/current connections to continue to old/current applications and new connections routed to new applications



Virtual Private Network

- Virtual Private Network (VPN) creates a direct and encrypted virtual channel over the Internet from an endpoint device to a network
- VPN uses different secured protocols
  - **Point-to-Point Tunneling (PPTP)**: first protocol with fast data speeds but basic encryption can be broken
  - **Layer 2 Tunnel / IPSec**: widely used protocol as replacement of PPTP and it is paired with security protocol IPsec for a strong security
  - **Internet Key Exchange v2**: creates a secure key exchange session and often paired with IPSec for encryption and authentication (e.g., Pfsense)
  - **Secure Socket Tunneling**: offers a strong security with 2048-bit SSL/TLS certificates for authentication and 256-bit SSL keys for encryption
  - **OpenVPN**: supports AES-256 bit key encryption with 2048-bit RSA authentication but has slower speeds

Virtual Private Network



Credits: Amazon

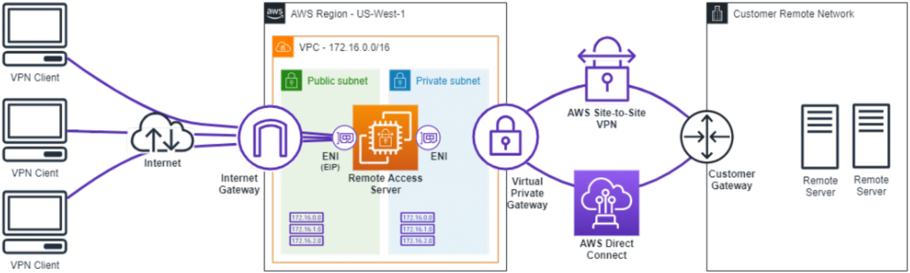
Virtual Private Cloud

- isolated, secured and private cloud in the public cloud
- It uses 4 components:
    - **Private Subnets**: have private IP address ranges making them unavailable to the public network
    - **Virtual LAN (VLAN)**: local network connected together without access to Internet
    - **VPN**: allowing to connect from a private network to the public network over an encrypted tunnel. To do so, it leverages the Network Address Translation and the Border Gateway Protocol (BGP) routing
- **What is the role of the Network Address Translation (NAT) ?**
- **What is the role of the BGP routing ?**

Virtual Private Cloud

- Network Address Translation
  - **Stateless**: maps private IP address to a public IP address without saving the public IPv4 address
  - **Stateful**: dynamically maps a private IP address to a public IP address from the NAT pool (group of public IPv4 addresses)
- Border Gateway Protocol (BGP) is a routing path-vector protocol used to exchange information across different network routers
  - a path vector sends the entire path for each destination based on policies or prefixes
  - the autonomous system boundary routers send path-vector messages (e.g., AS path, next-hop, origin) to notify the reachability of networks
  - Each router receives a path-vector message, verify it, update its routing table with the message according to its policy, and notify the nearest router.

Virtual Private Cloud

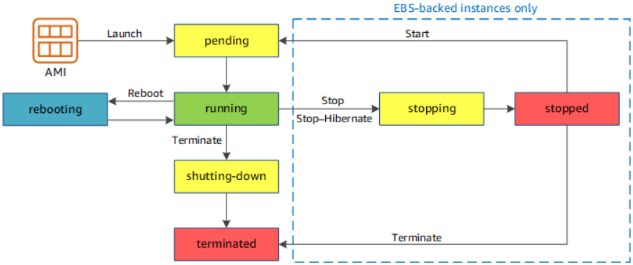


Credits: Amazon

Sondage ☺: https://app.wooclap.com/AOKAYY.

Elastic Compute Cloud

- EC2 is a service that uses the concept of instances based on virtual machines
- It specifies hardware, compute, memory, storage capabilities
- It manages instances in the cloud: launching, pending, running, stopping, termination



Credits: Amazon