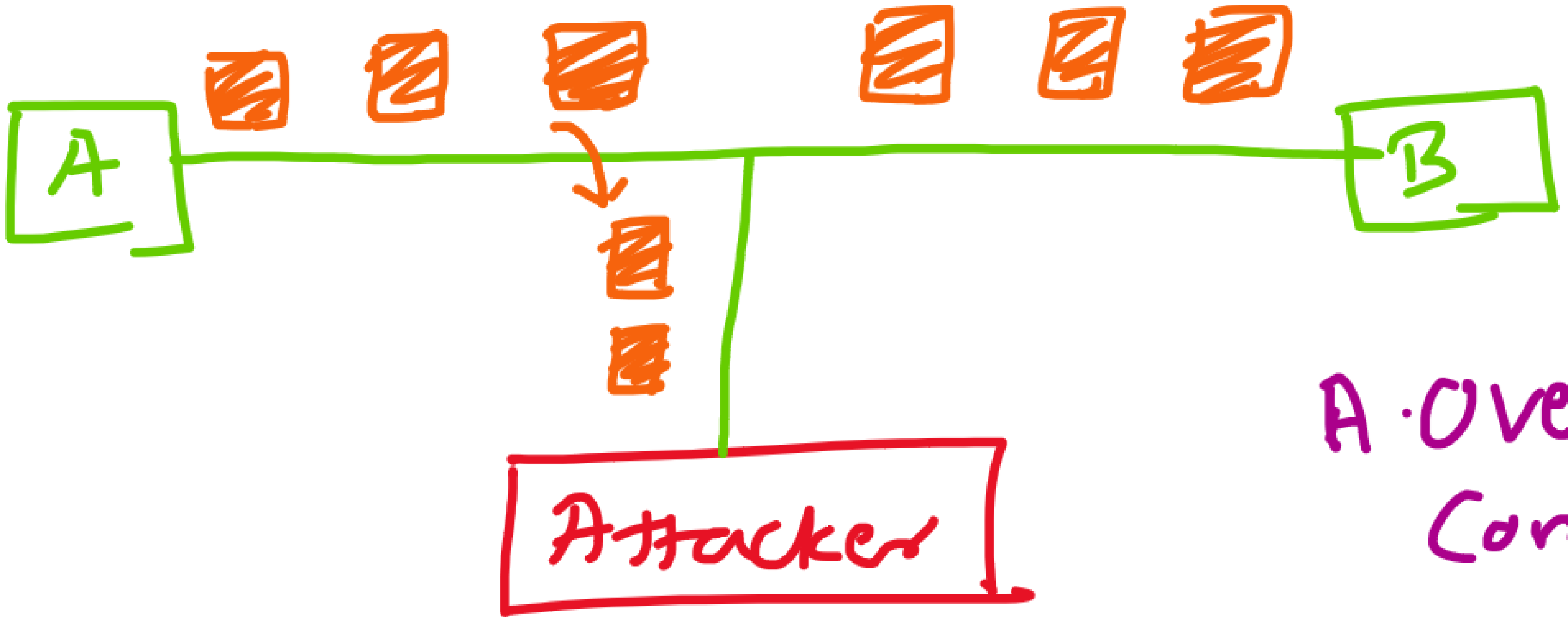
VIT Vidyalankar Institute of Technology
Accredited A+ by NAAC

CSS

Prof. Amit K. Nerurkar
Assistant Professor
Department of Computer Engineering
Vidyalankar Institute of Technology, Wadala

① Packet Sniffing:

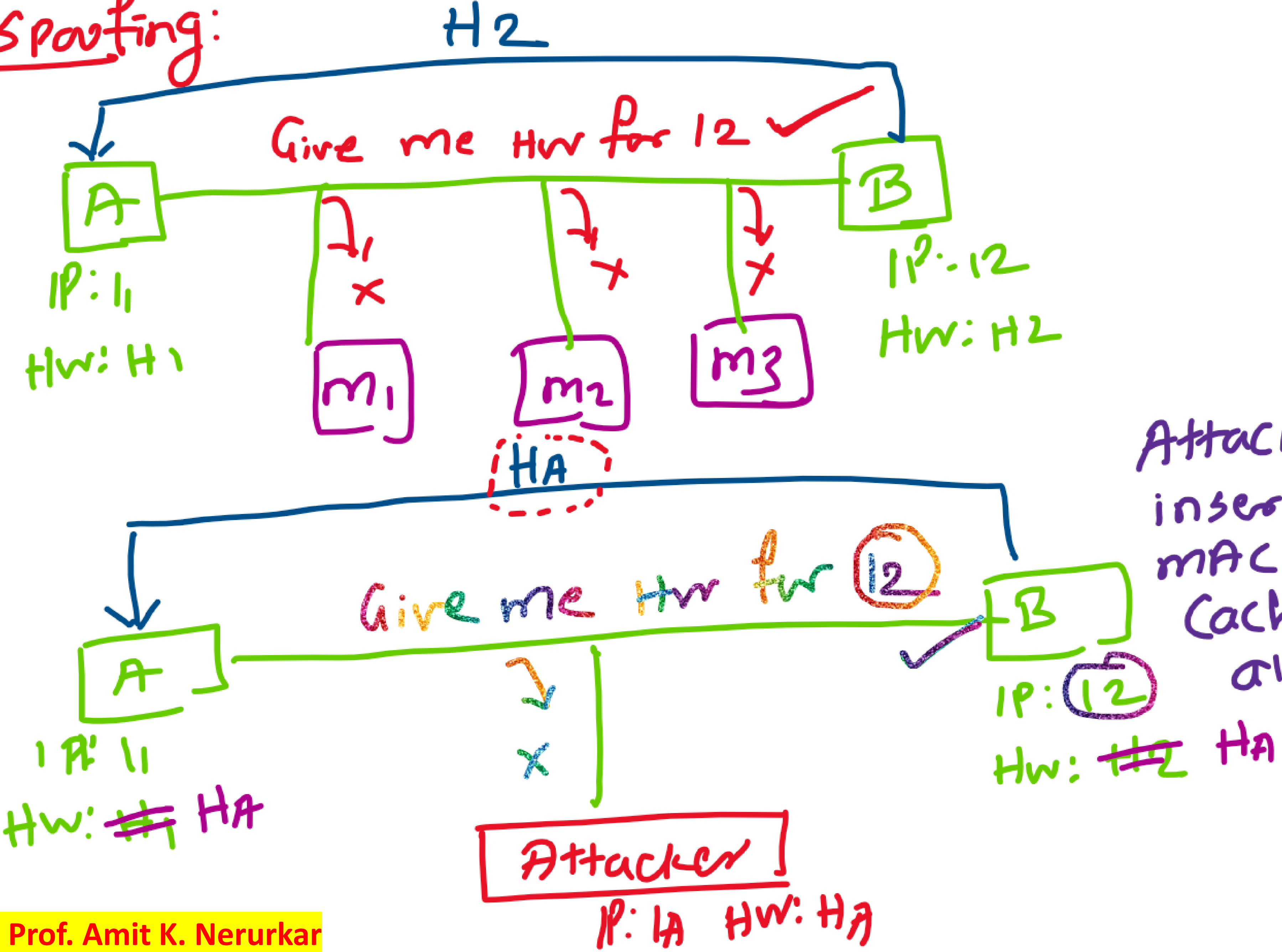


A. Overhearing the Comm.

Protection:

① Cryptography (Enc & Dec)

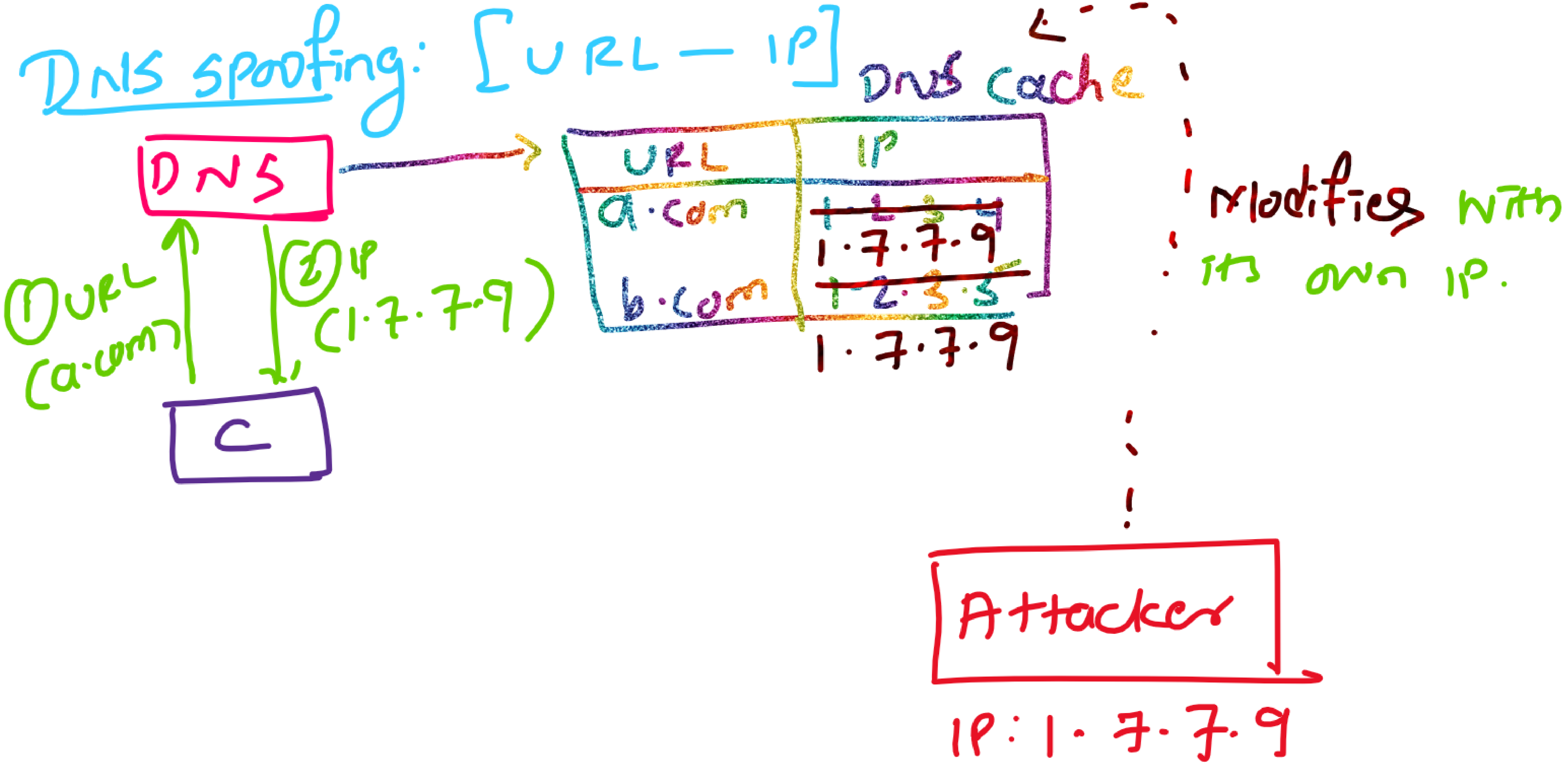
ARP spoofing:



Attacker intentionally inserts its own MAC (HW) add. in cache table of all machines.

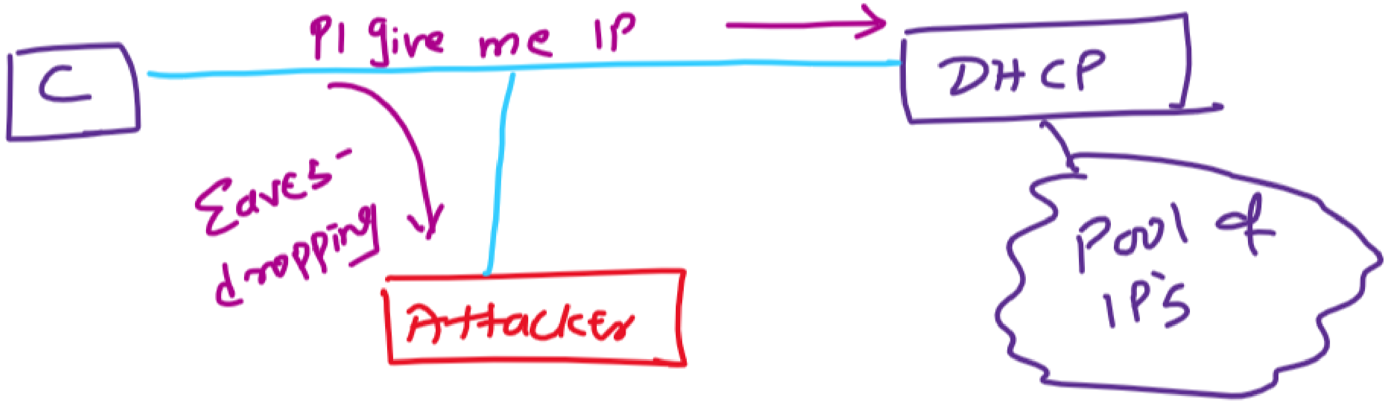
Prepared by Prof. Amit K. Nerurkar

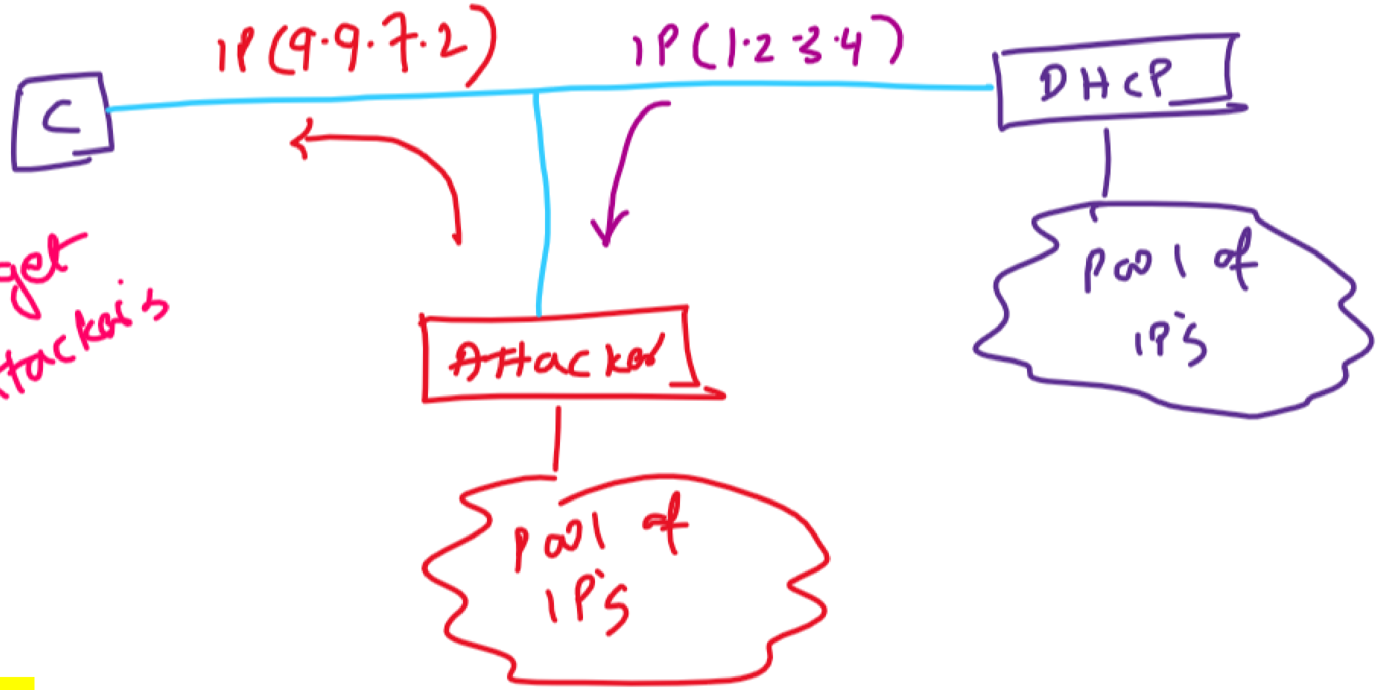
DNS spoofing: [URL — IP]



URL	IP
a.com	~~1.2.3.4~~ 1.7.7.9
b.com	~~1.2.3.5~~ 1.7.7.9

③ DHCP Spoofing:





Client will get IP & attacker's N/w.

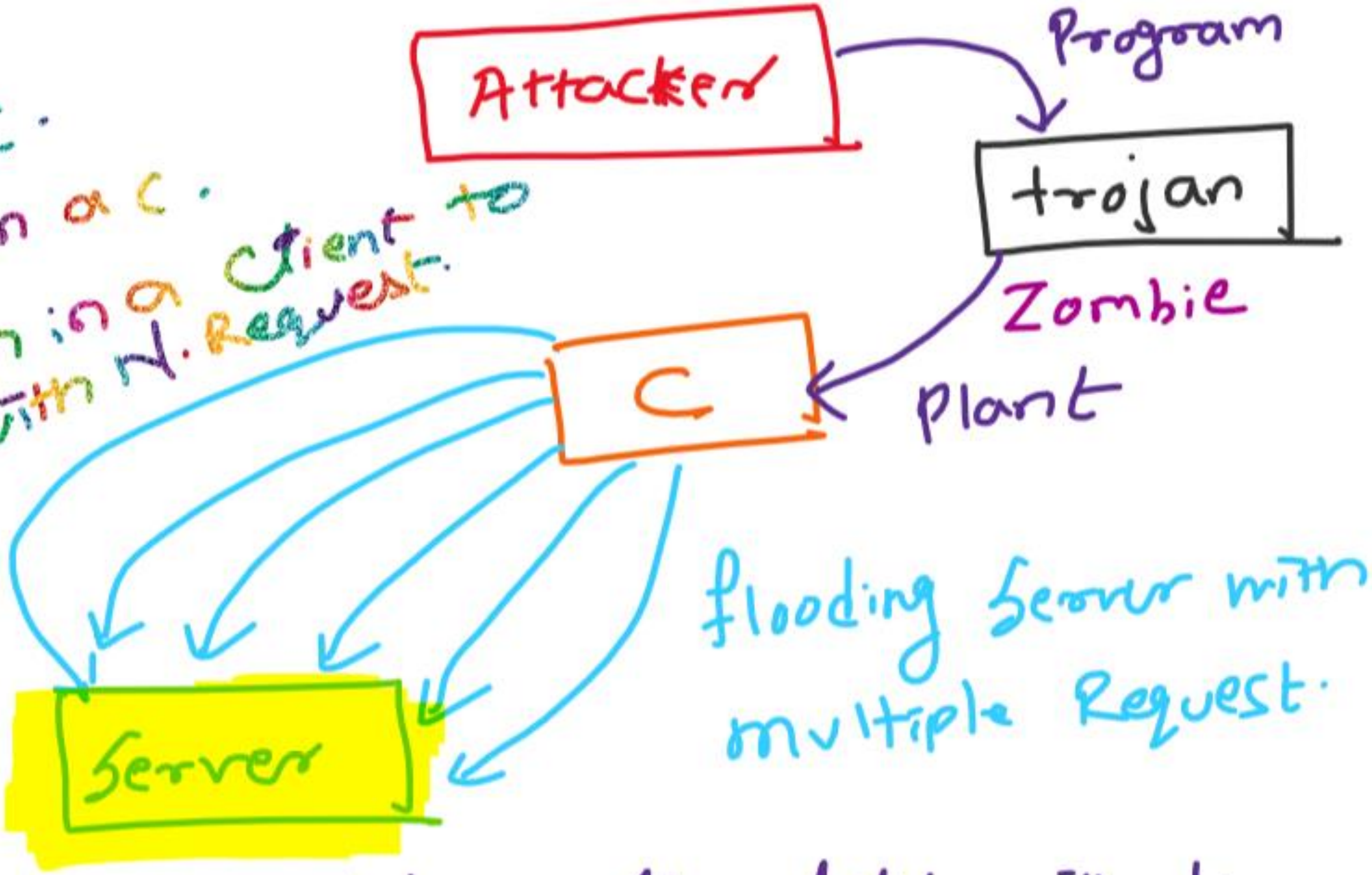
1) Progam a trojan

2) IP spoofing of C.

3) Plant a trojan in a C.

4) Signal a trojan in a client to find server with N. Request.

5) DOS.

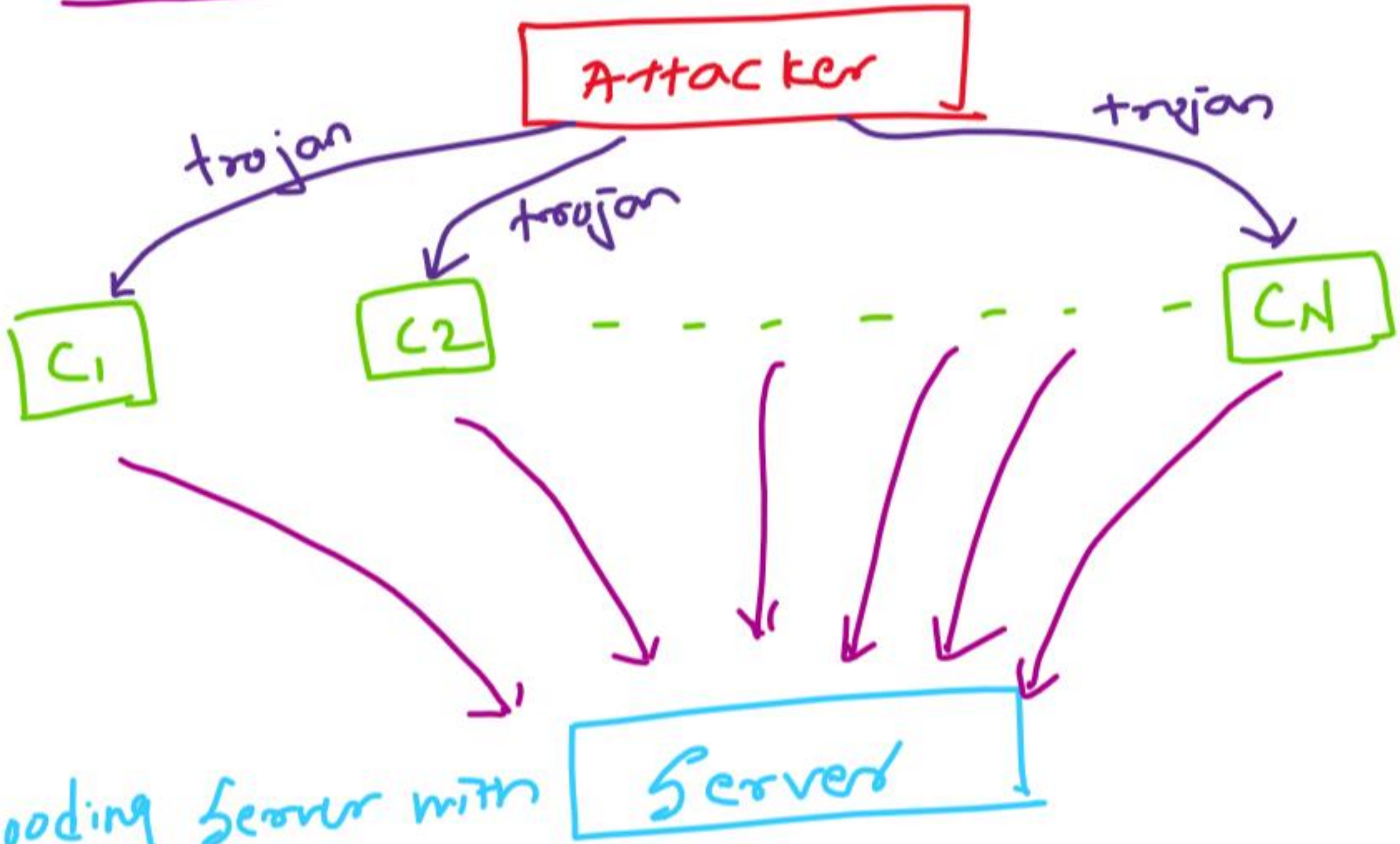


flooding server with multiple Request.

Overloaded & ultimately will deny service. (DOS)

Now, server will block client using firewall-

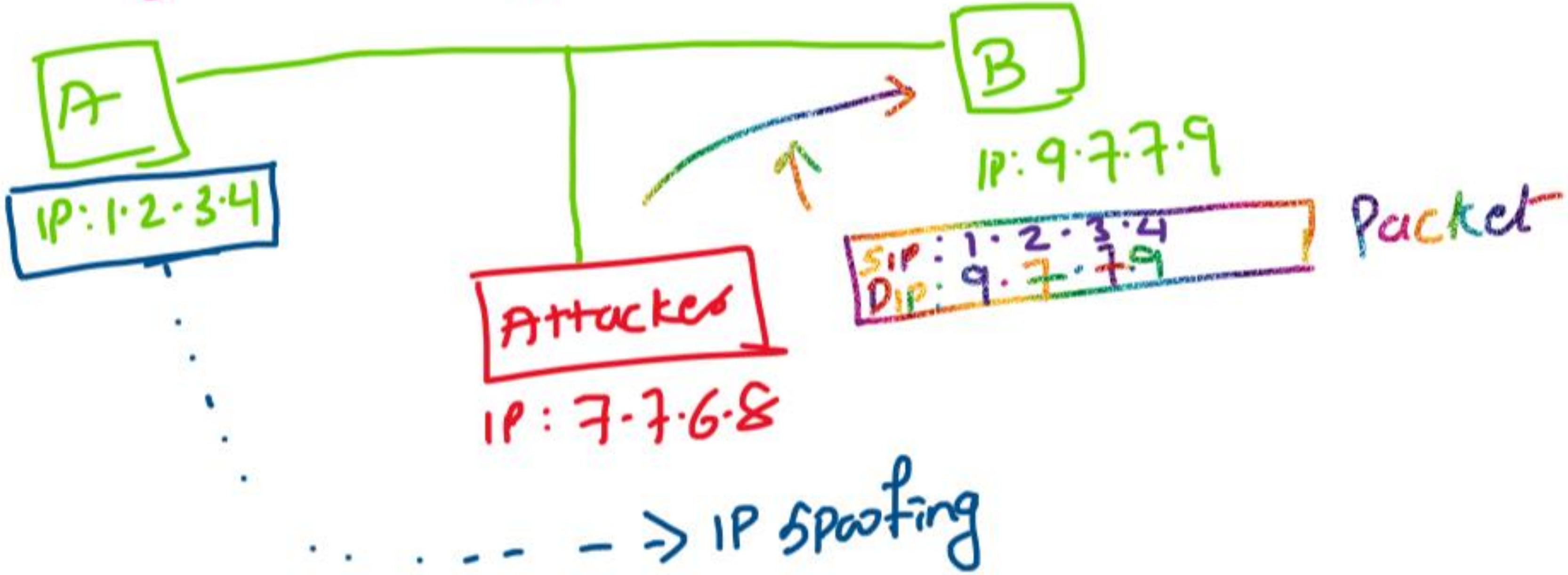
DDos: Distributed DOS:



flooding server with multiple Request from multiple clients.

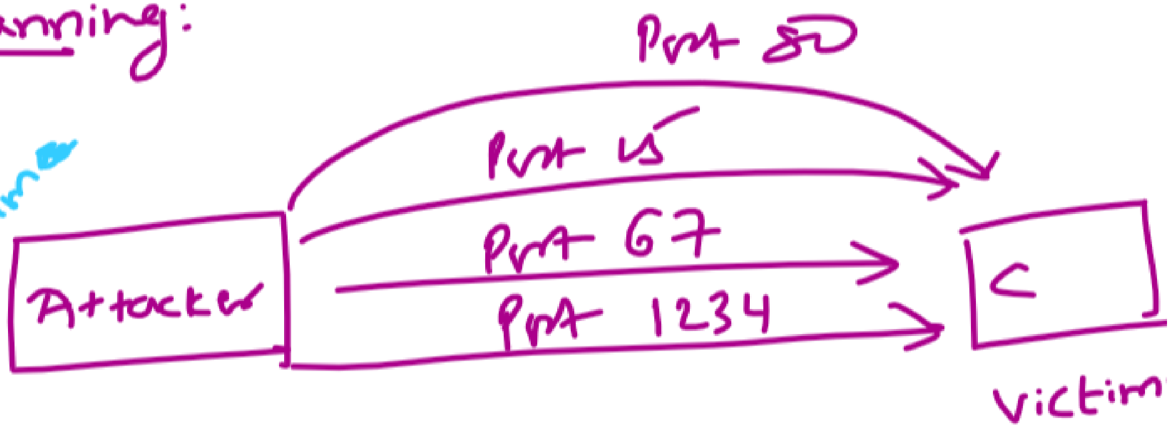
ill Stop DoS.

(i) IP Spoofing: Stealing the IP address.



Port Scanning:

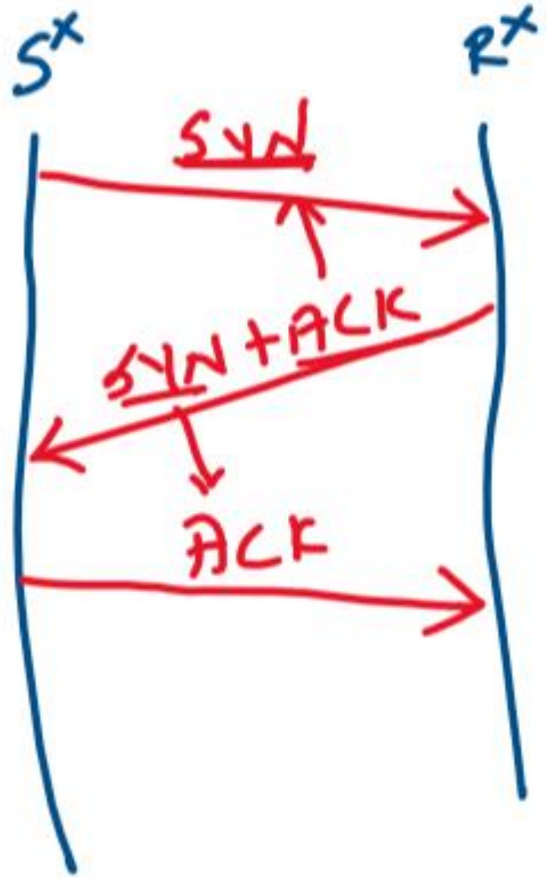
ying to identify which ports of victim open.

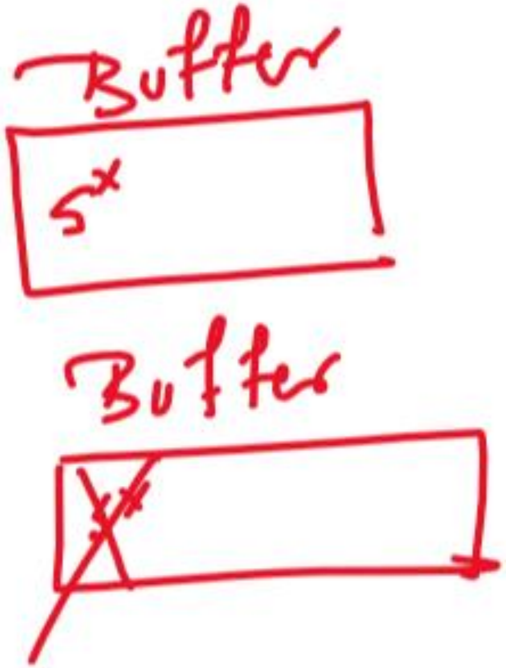


anc

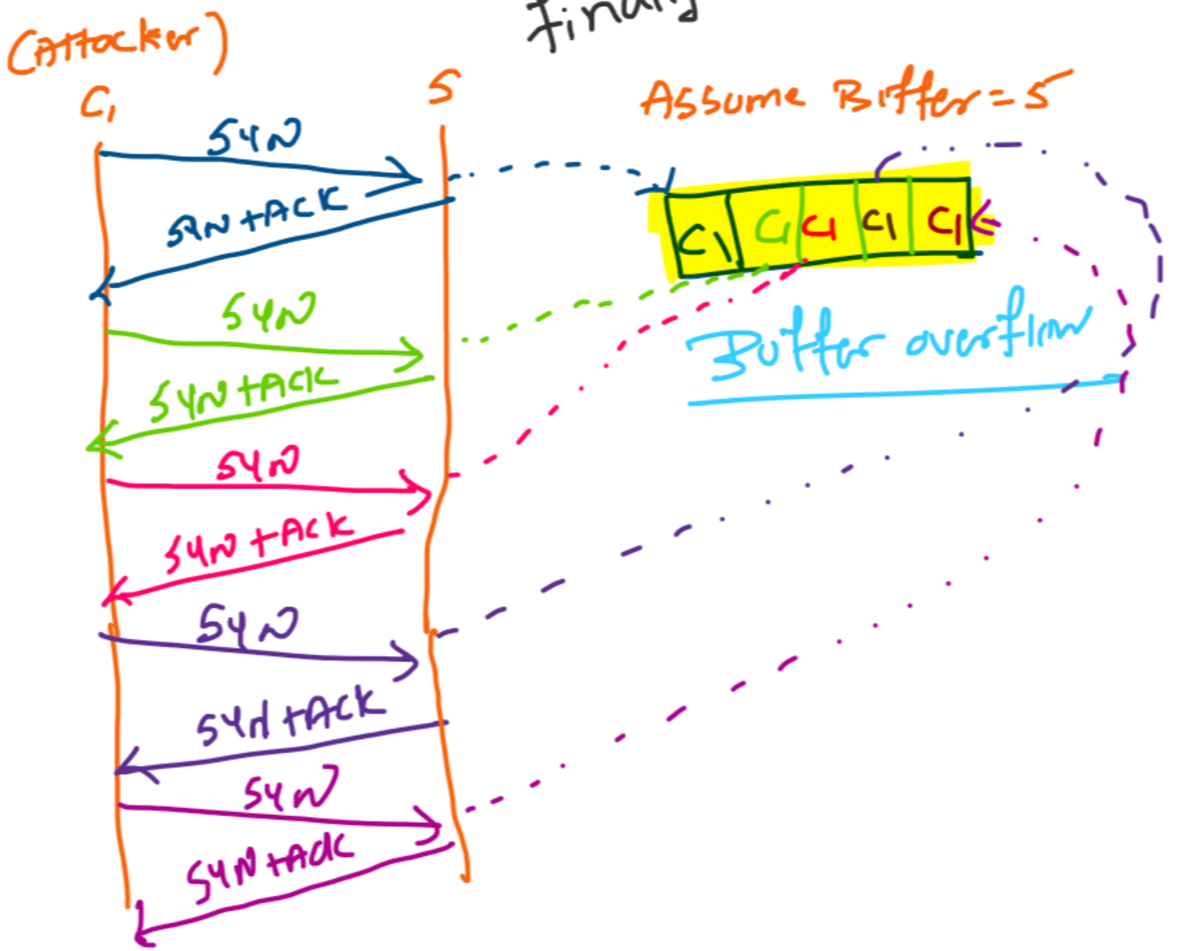
SYN flooding:

3-way handshaking

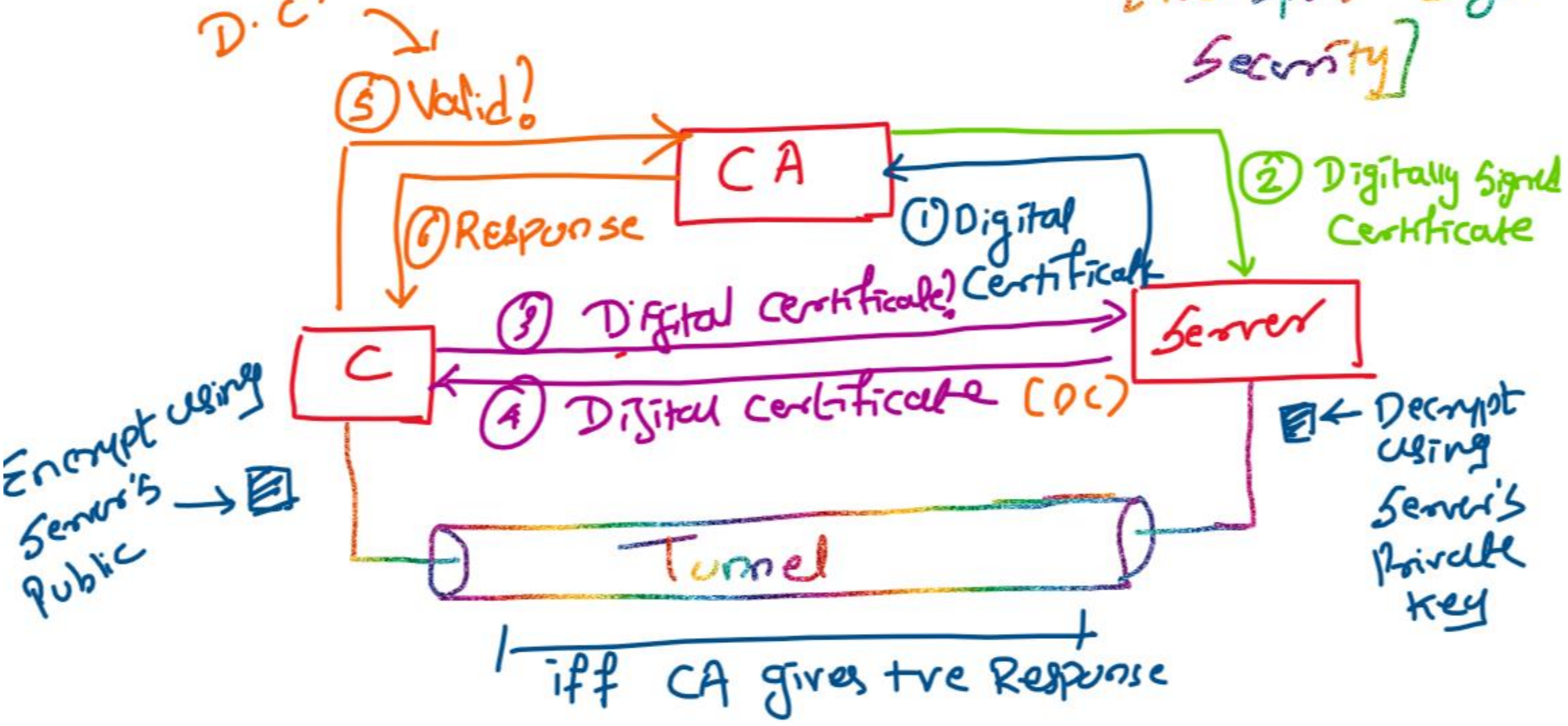




Intentionally C1 will not send ACK & this will make buffer full, finally S will cause DoS.



SSL [Secure Socket Layer] → TLS [Transport Layer Security]

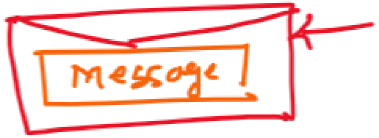

D.C'
5 Valid?
CA
6 Response
1 Digital Certificate
2 Digitally Signed Certificate
3 Digital certificate?
C
Server
4 Digital certificate (DC)
Encrypt using Server's Public
Decrypt using Server's Private key
Tunnel
iff CA gives +ve Response

PGP [Pretty Good Privacy]

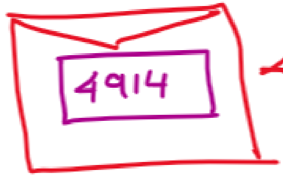
L Email communication.

Sx

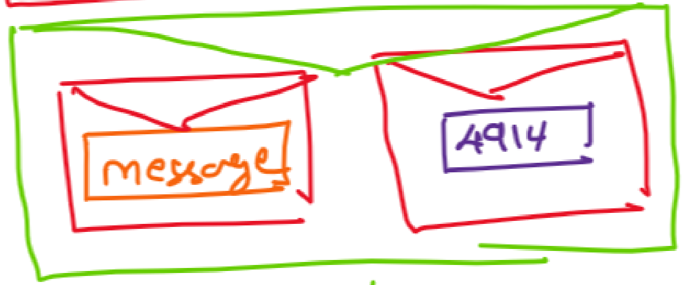
① Message ② Generate a Random key = 4914

③


Encrypted using 4914

④


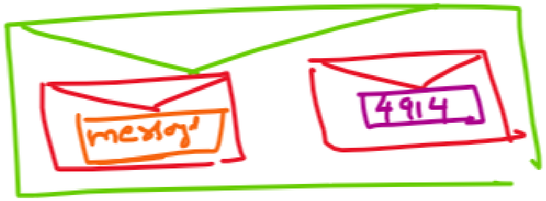
Encrypt using R^x Public key

⑤


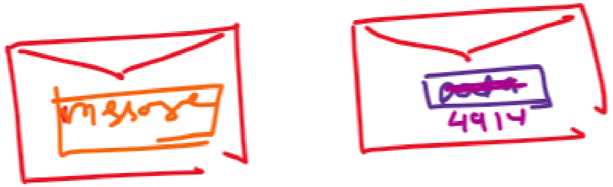
Send this message to R^x

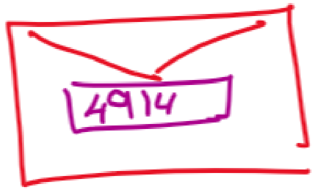
Data

Rx

①


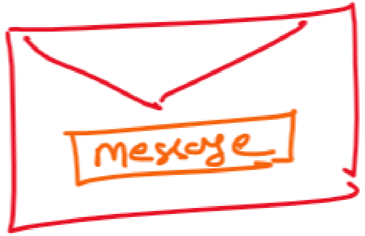
Data



②


Decrypt using R^x Private key

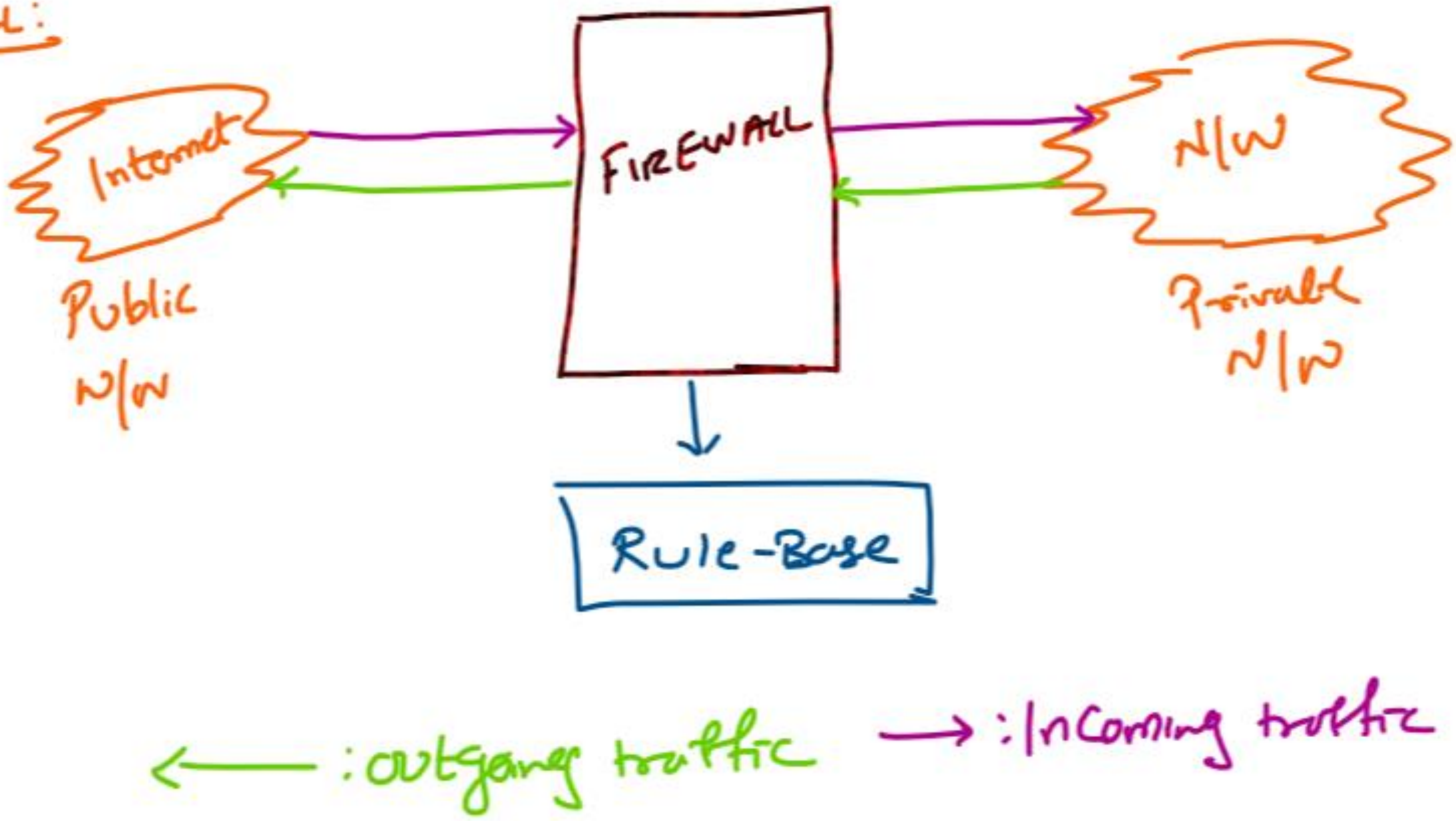
4914

③


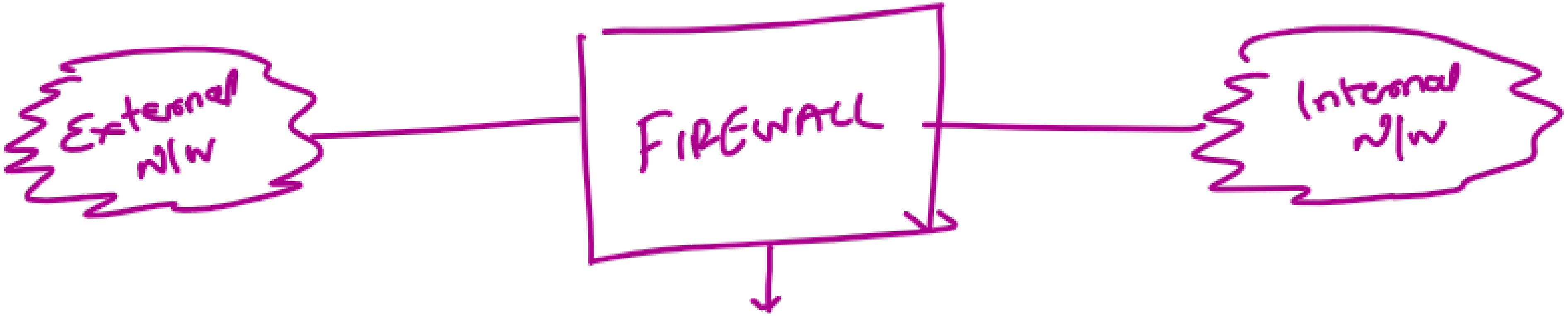
Decrypt using 4914

message

FIREWALL:


Internet
Public N/W
FIREWALL
N/W
Private N/W
Rule-Base
← : outgoing traffic
→ : Incoming traffic

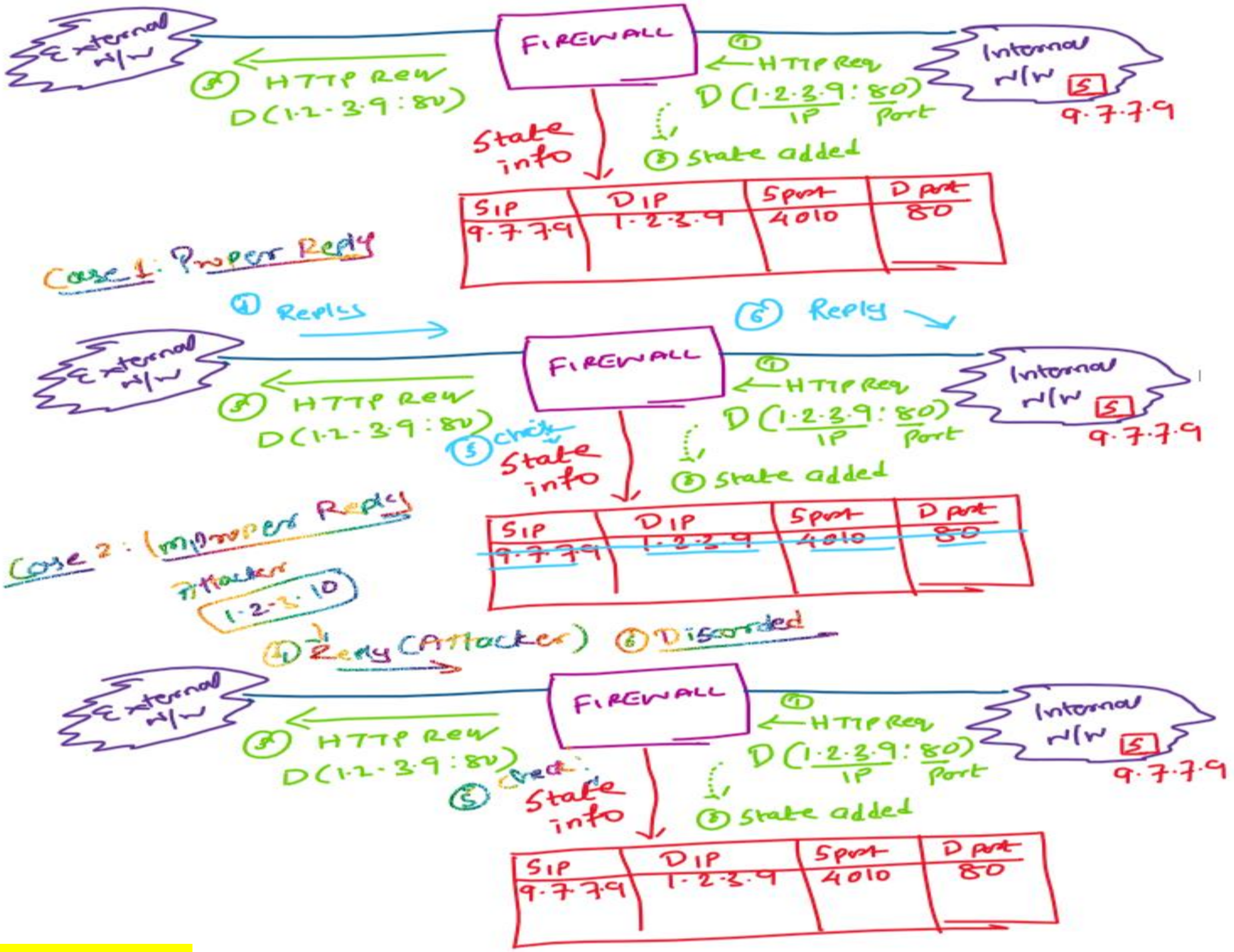
① Packet filtering firewall [Based on Rulebase allow or block the Packets]



FOR	SIP	DIP	Sport	Dport	action
IN	1.2.3.4	ANY	ANY	ANY	DROP
OUT	ANY	1.2.3.4	ANY	ANY	DROP

Issue: Doesn't maintain any state.

2) Stateful Inspection : Before sending Request the Packet's Info is maintained is state.

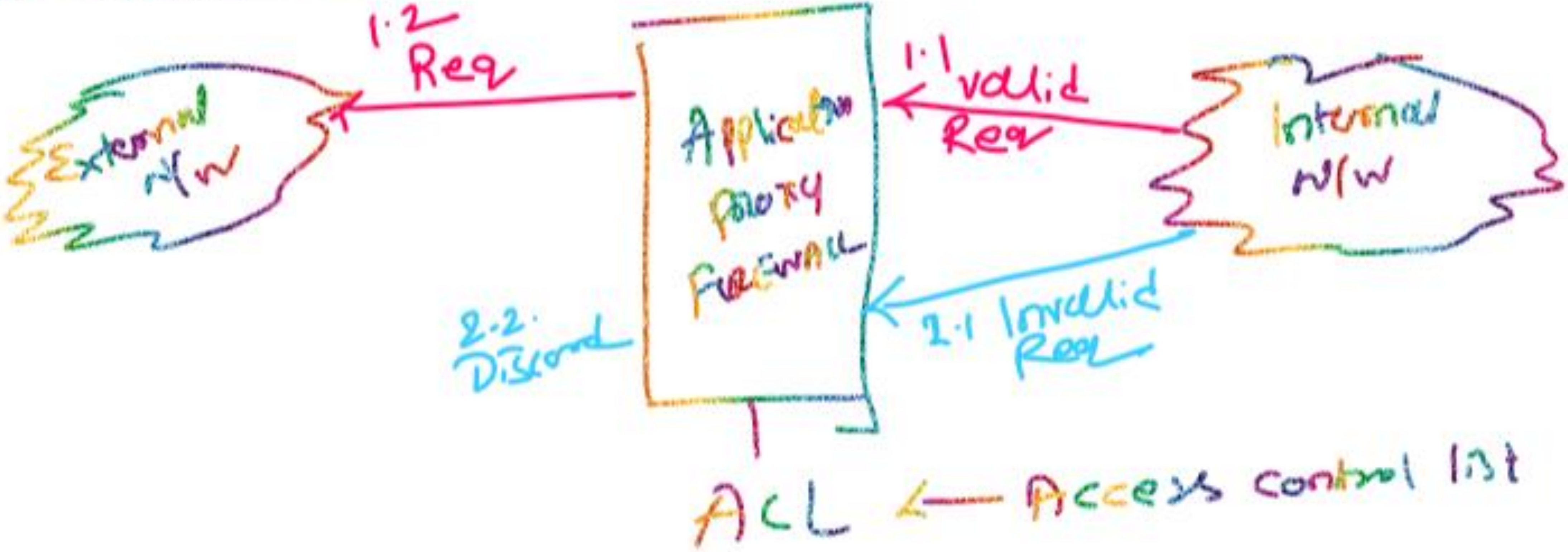


SIP	DIP	Sport	D port
9.7.7.9	1.2.3.9	4010	80

SIP	DIP	Sport	D port
9.7.7.9	1.2.3.9	4010	80

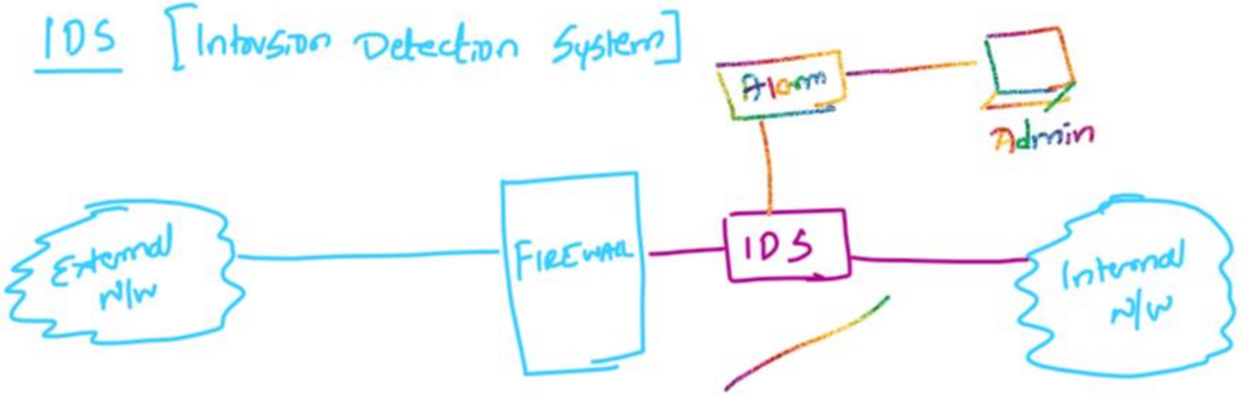
SIP	DIP	Sport	D port
9.7.7.9	1.2.3.9	4010	80

3 Application Proxy:



Passive

IDS [Intrusion Detection System]



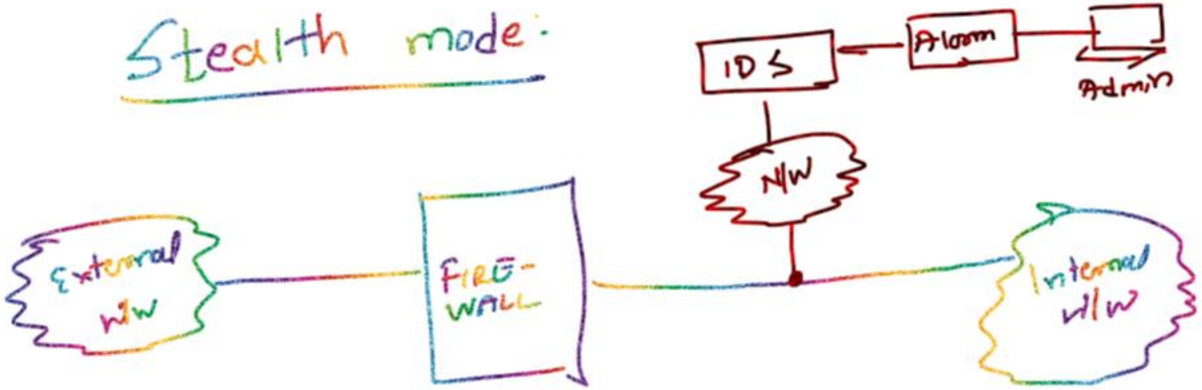
① Signature

eg SYN Flooding, Virus

② Heuristic [Anamoly]

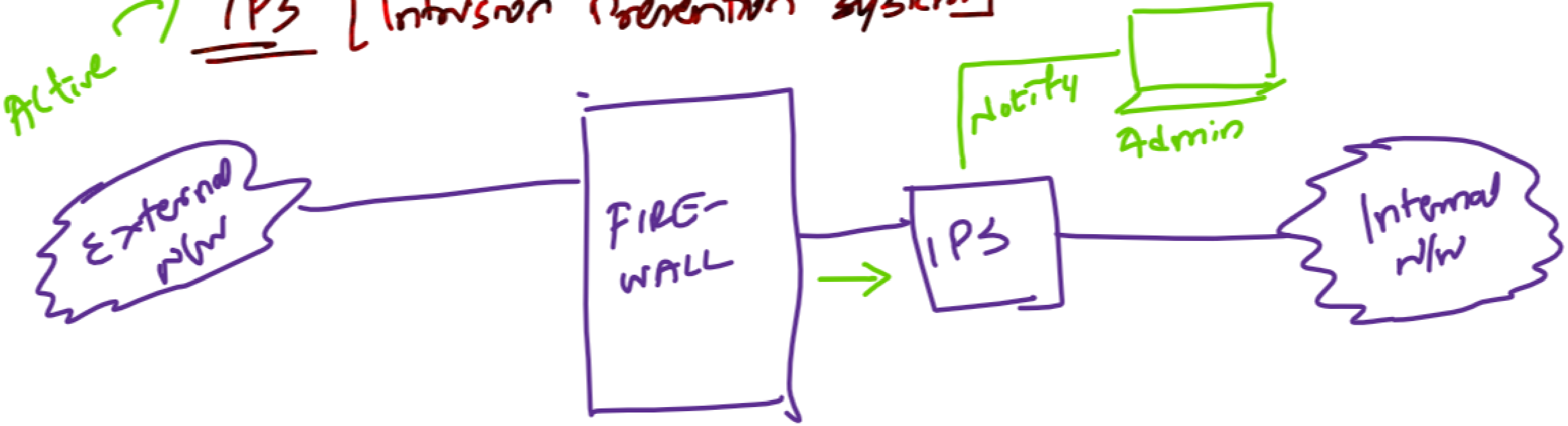
→ Behaviour

Stealth mode:



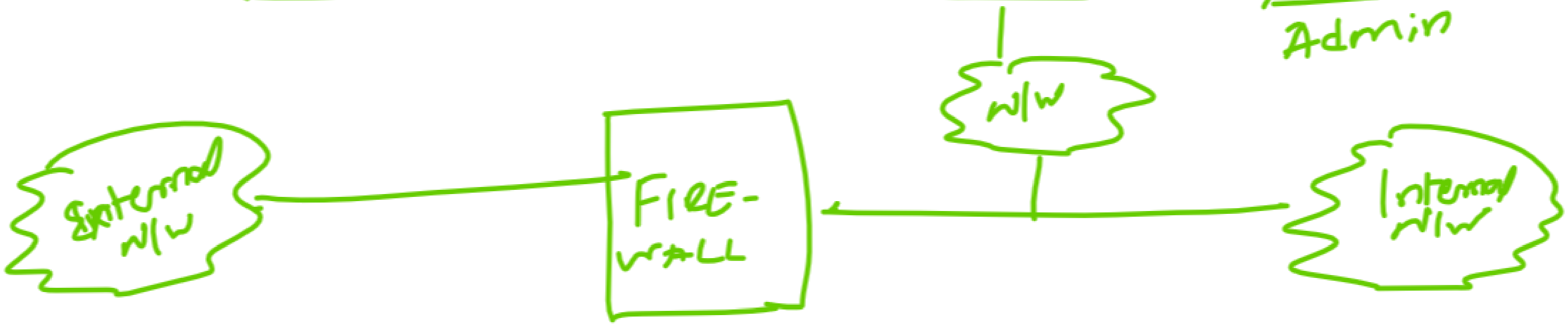
IDS shifted to some other N/W so that it is hidden

Active → **IPS** [Intrusion Prevention system]

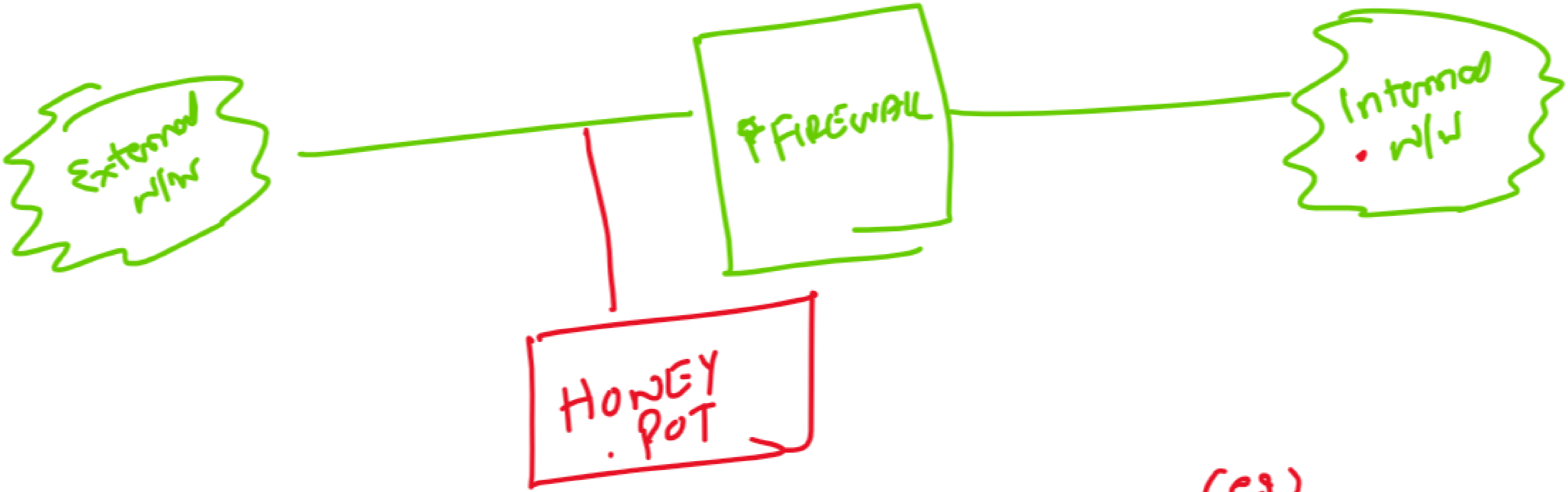


IPS: If it realizes that Incoming traffic contains attack like Signature, block it & inform Admin.

Stealth mode IPS:



HONEYPOT



Device that mimic like original website (eg) to attract the attacker.

Thank You

Name: Amit K. Nerurkar

Designation: Assistant Professor

College: Vidyalankar Institute of Technology