CPR E 431

BASICS OF INFORMATION SYSTEM SECURITY

Firewall and Intrusion Prevention System

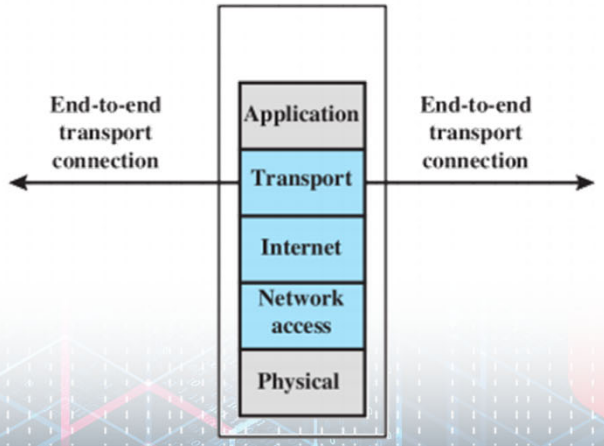
Packet Filtering Firewall

Video Summary

- What is Packet filtering firewall?
- Packet Filtering Rules
- Example of Packet Filtering Firewalls
- Example Network

Packet Filtering Firewall

- Security policy implemented by set of rules
- Rules define which packets can pass through the firewall
- Firewalls inspects each arriving packet (in all directions), compares against rule set, and takes action based on matching rule
- Default policies: action for packets for which no rule matches
  - Accept (allow, forward)
  - Drop (reject, discard) - recommended

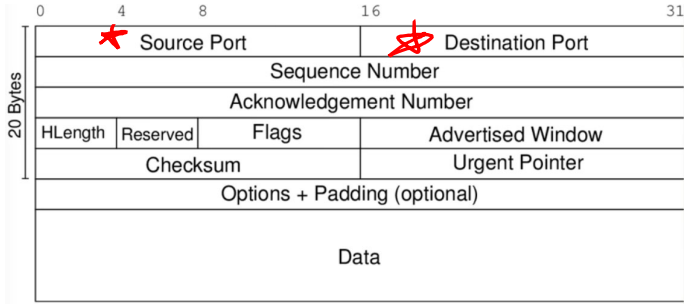


Packet Filtering Rules

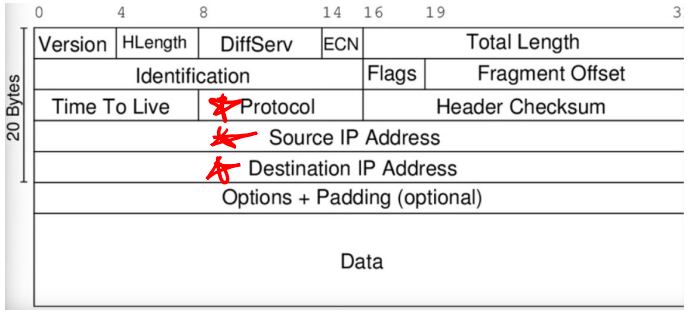
Packet Information

- IP address: identifies host or network
- Port number: identifies server, e.g. web (80), email (25)
- Protocol number: identifies transport protocol, e.g. TCP or UDP
- Firewall interface: identifies immediate source/destination
- Other transport, network, data link packet header fields

TCP



IP



Rules

- Conditions defined using packet information, direction
- Wildcards (*) support to match multiple values
- Actions typically accept or drop
- List of rules processed in order

Example Packet Filtering Firewalls

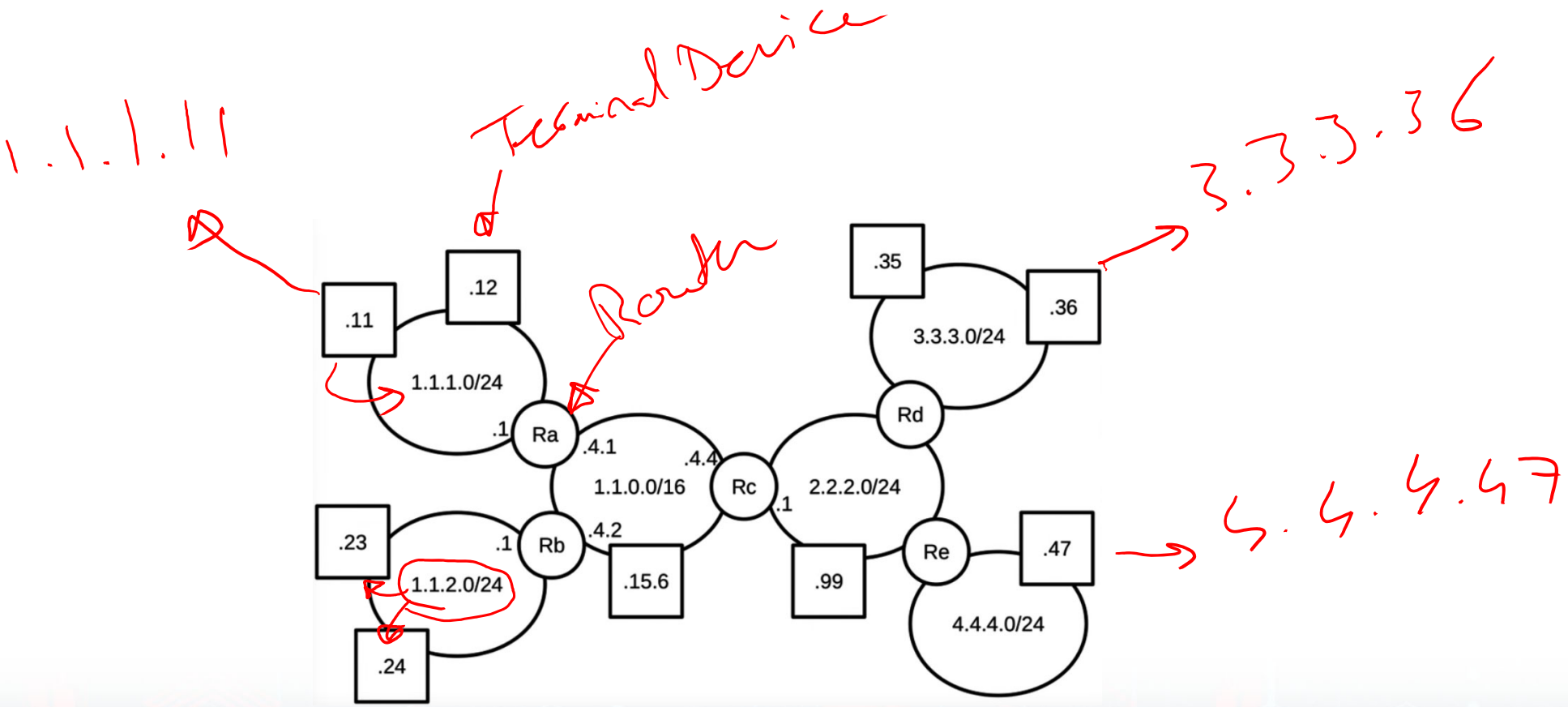
Software

- In operating systems: iptables (Linux), ipfw (Mac OSX), pf (BSD), Windows Firewall
- Standalone software: Comodo, Kaspersky, Norton, ZoneAlarm, Check Point, ...

Appliances

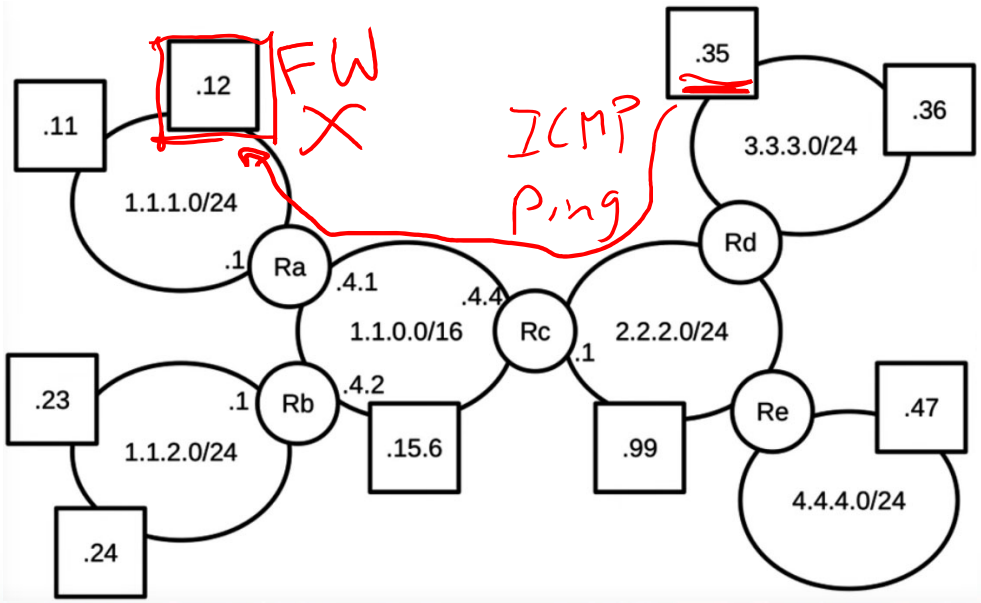
- Firewall included in most consumer and enterprise routers
- Dedicated hardware: Cisco ASA/PIX, Dell SonicWALL, HP, Barracuda, Juniper, ...
- Dedicated software distributions: pfSense, Monowall, Smoothwall, ClearOS, Untangle, IPCop, ...

Example Network



Example Network

Suppose we have a firewall running on computer 1.1.1.12
Aim is to stop computer 3.3.3.35 from pinging 1.1.1.12

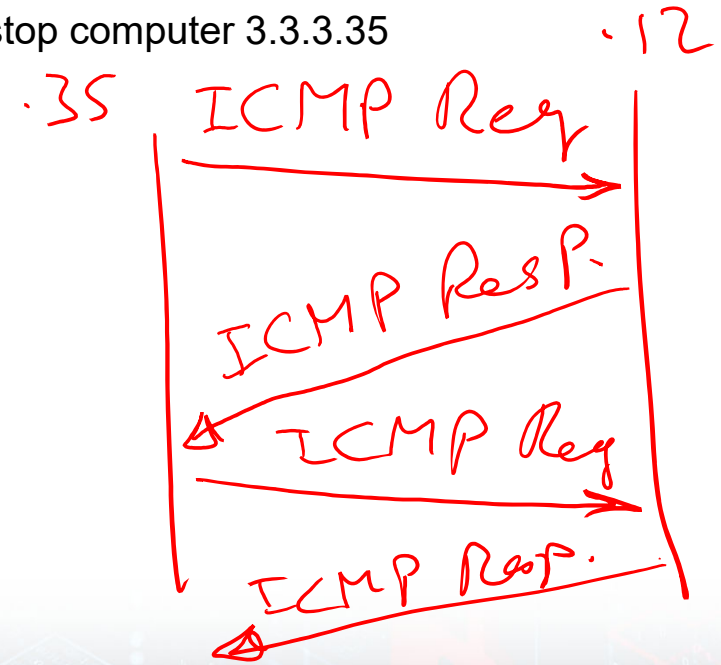


Example Network

Suppose we have a firewall running on computer 1.1.1.12
Aim is to stop computer 3.3.3.35 from pinging 1.1.1.12

How ping works?

How firewall can stop computer 3.3.3.35

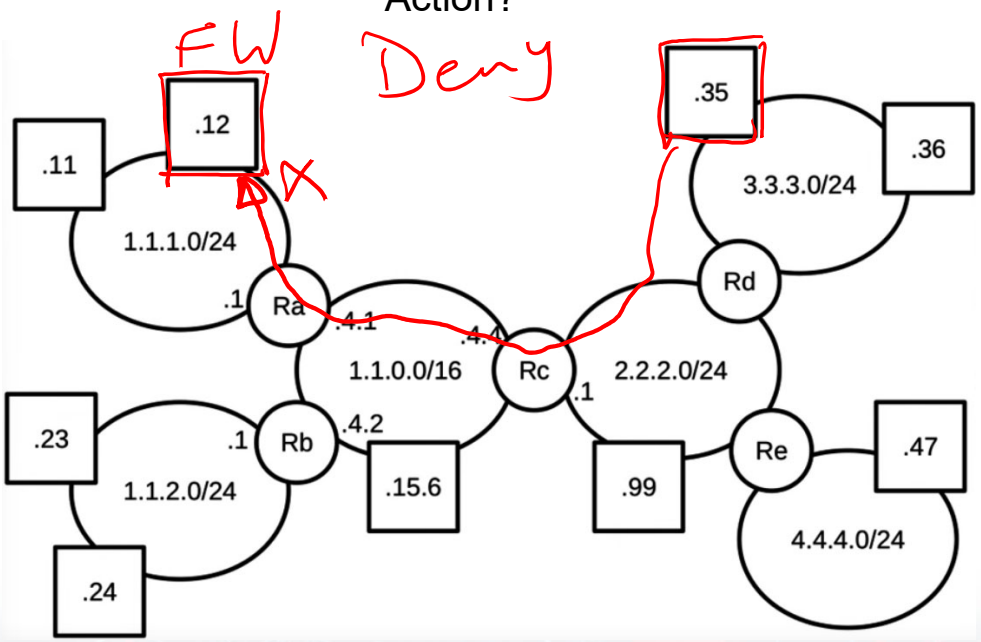


Example Network

Suppose we have a firewall running on computer 1.1.1.12
Aim is to stop computer 3.3.3.35 from pinging 1.1.1.12

SrcIP= 3.3.3.35 SrcPort= * Protocol= ICMP (1)
DstIP= 1.1.1.12 DstPort= *

Action?



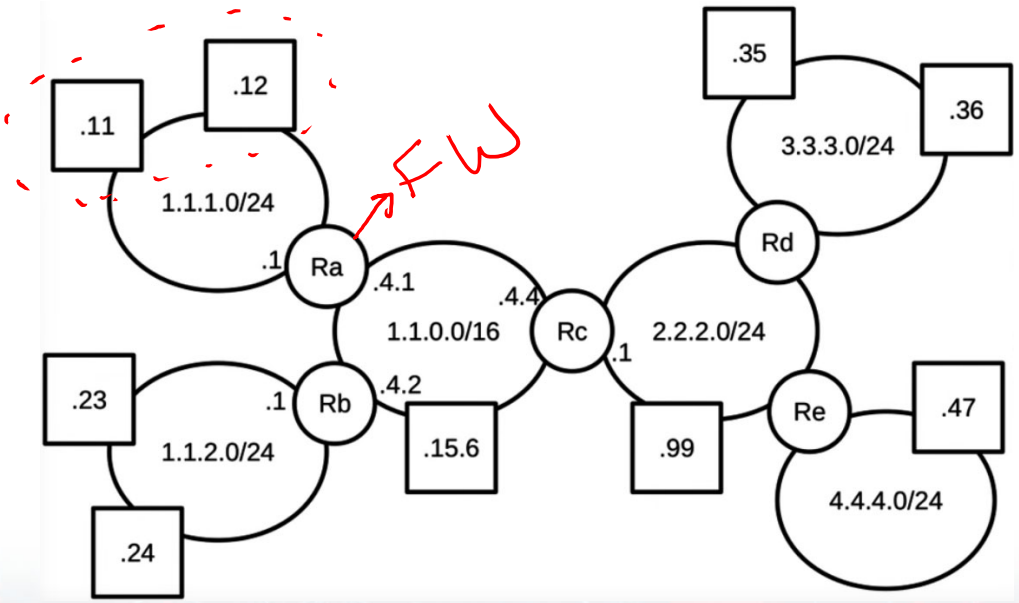
Default Allow Accept

Example Network

What if we moved the firewall from computer 1.1.1.12 to Ra then we now want to protect subnet 1.1.1.0/24 from pinging

SrcIP= * SrcPort= * Protocol= 1 → ICMP

DstIP= 1.1.1.0/24 DstPort= *



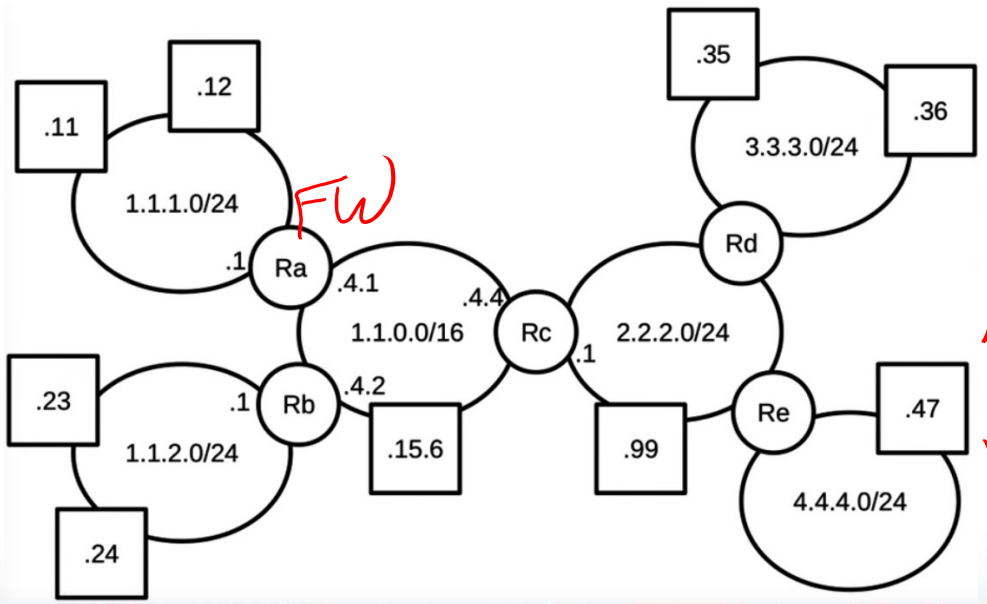
Action:
Deny
Default:
Accept

Example Network

What if we moved the firewall from computer 1.1.1.12 to Ra
Aim: prevent outsiders from SSHing 1.1.1.11

SrcIP= * SrcPort= * Protocol= *
DstIP= 1.1.1.12 DstPort= 22

6 17



SSH → UDP
→ TCP

Action: Drop
Default: Accept

Example Network

```
$ less /etc/services
telnet          23/tcp
smtp            25/tcp          mail
time            37/tcp          timserver
time            37/udp          timserver
rlp             39/udp          resource
nameserver      42/tcp          name
whois           43/tcp          nicname
tacacs          49/tcp
l (TACACS)
tacacs          49/udp
re-mail-ck      50/tcp
ng Protocol
re-mail-ck      50/udp
domain          53/tcp
domain          53/udp
```

```
$ less /etc/services
tcpmux          1/tcp
ultiplexer
echo            7/tcp
echo            7/udp
discard         9/tcp           sink null
discard         9/udp           sink null
systat          11/tcp          users
daytime         13/tcp
daytime         13/udp
netstat         15/tcp
qotd            17/tcp          quote
msp             18/tcp
col
msp             18/udp
chargen         19/tcp          ttytst source
chargen         19/udp          ttytst source
ftp-data        20/tcp
ftp             21/tcp
fsp             21/udp          fspd
ssh             22/tcp
rotocol
ssh             22/udp
```

Table 9.1

Packet-Filtering Examples

Rule	Direction	Src address	Dest addresss	Protocol	Dest port	Action
1	In	External	Internal	TCP	25	Permit
2	Out	Internal	External	TCP	>1023	Permit
3	Out	Internal	External	TCP	25	Permit
4	In	External	Internal	TCP	>1023	Permit
5	Either	Any	Any	Any	Any	Deny

Video Summary

- What is Packet filtering firewall?
- Packet Filtering Rules
- Example of Packet Filtering Firewalls
- Example Network