Network Defenses

KAMI VANIEA

21 JANUARY

Similar statements are found in most content hosting website privacy policies.

What is it about how the internet works that makes this statement necessary to have?

"By submitting, posting or displaying User Content on or through the Service, you grant Piazza a worldwide, non-exclusive, royalty-free license (with the right to sublicense) to use, copy, reproduce, process, adapt, modify, publish, transmit, display and distribute such User Content. This license is limited to providing the Service. Your User Content will not be used for publicity, advertising or any public statements without your prior consent."

-- Piazza Terms of Service

First, the news…

- The silencing of KrebsOnSecurity opens a troubling chapter for the Internet

- http://arstechnica.co.uk/security/2016/09/why-the-silencing-of-krebsonsecurity-opens-a-troubling-chapter-for-the-net/

Tutorials

- Tutorials start in week 3

- Path is wrong

- The ITO currently has 13 tutorials for this course when they should have 5 tutorials and 5 labs.

- We are trying **really** hard to get this sorted by next week
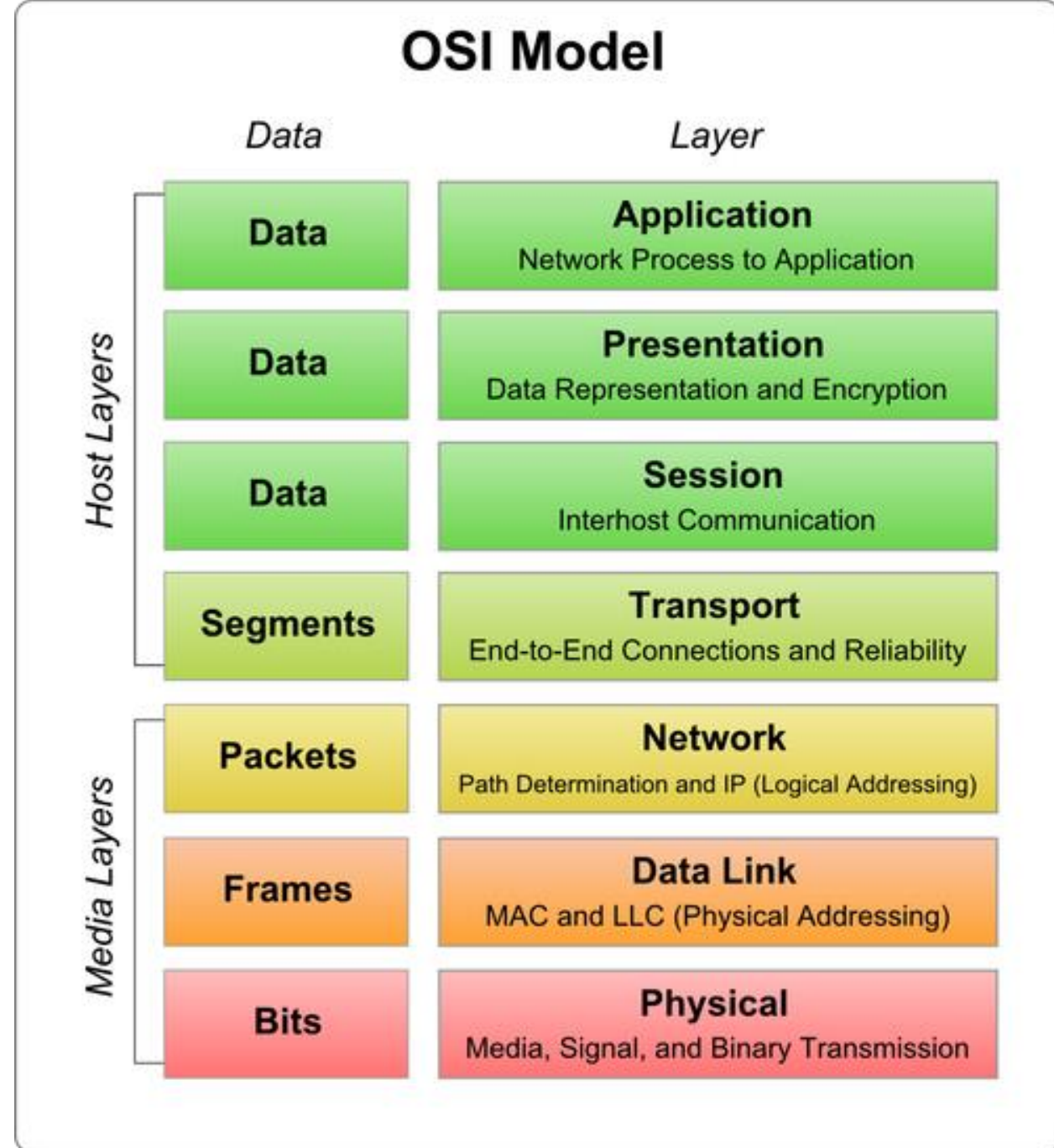
Courseworks

- There are three courseworks

- Deadlines are on the website

- The deadlines the ITO has are wrong, again we are working to get this resolved
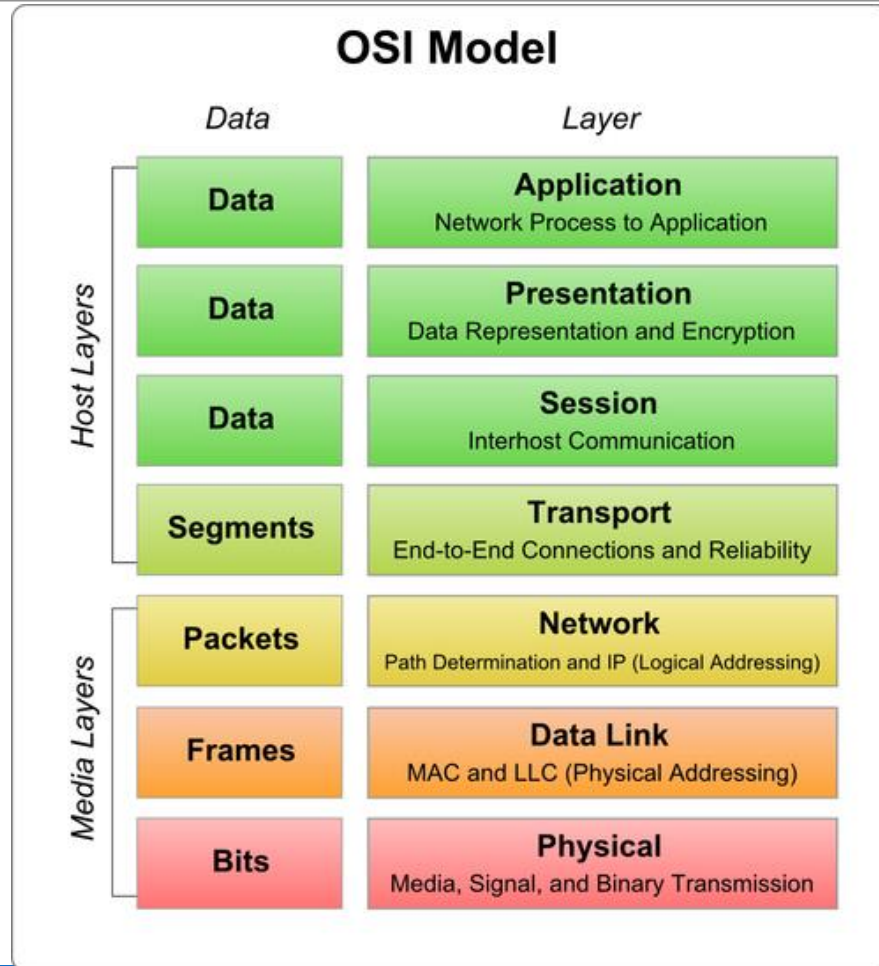
Today

- Open System Interconnect (OSI) model

- Firewalls

- Intrusion detection systems (IDS)

- Time allowing:
  - Network Address Translation (NAT)

Open Systems Interconnect model

- A good way to think about networking steps logically
- Not how software is actually built

OSI Model

Data	Layer
Data	**Application** — Network Process to Application
Data	**Presentation** — Data Representation and Encryption
Data	**Session** — Interhost Communication
Segments	**Transport** — End-to-End Connections and Reliability
Packets	**Network** — Path Determination and IP (Logical Addressing)
Frames	**Data Link** — MAC and LLC (Physical Addressing)
Bits	**Physical** — Media, Signal, and Binary Transmission

Host Layers: Application, Presentation, Session, Transport

Media Layers: Network, Data Link, Physical

OSI in terms of debugging errors

Can your browser open another website?

Do you have a viewer that supports jpg (image format)?

Can you ping the webserver you are trying to reach?

Can you ping the gateway or DNS server?

Do you have an IP address?

Is the light on the modem on?

Is the network cable plugged in?

Sender:
Apache server

Recipient:
Firefox user

7		**Application** — Network process to application
6		**Presentation** — Data representation and encryption
5		**Session** — Interhost communication
4		**Transport** — End-to-end connection and reliability
3		**Network** — Path determination and IP (Logical Addressing)
2		**Data Link** — MAC and LLC (Physical Addressing)
1		**Physical** — Media, signal, and binary transmission

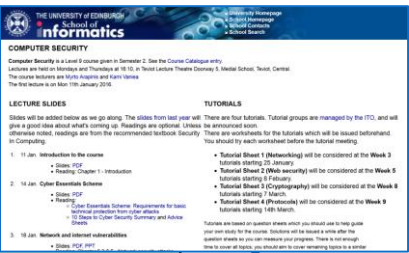Data starts at the top of the OSI stack at level 7.

It progresses down the stack with each successive level adding or changing information.

At level 1 it travels across the physical layer to the recipient computer.

The recipient then processes the data up the stack. At level 7 an application processes the data.
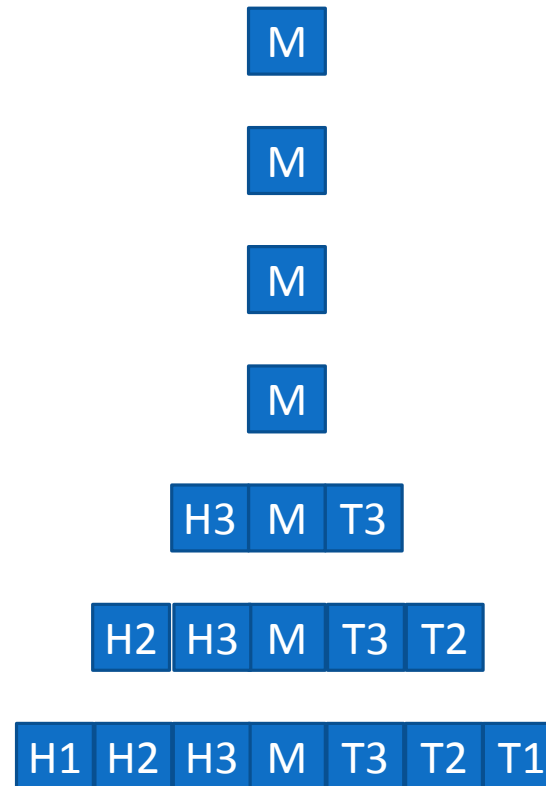
7		**Application** — Network process to application
6		**Presentation** — Data representation and encryption
5		**Session** — Interhost communication
4		**Transport** — End-to-end connection and reliability
3		**Network** — Path determination and IP (Logical Addressing)
2		**Data Link** — MAC and LLC (Physical Addressing)
1		**Physical** — Media, signal, and binary transmission

- Levels 7 and 6 involve the internal representation of the message
- Levels 5 and 4 involve setting up the connection
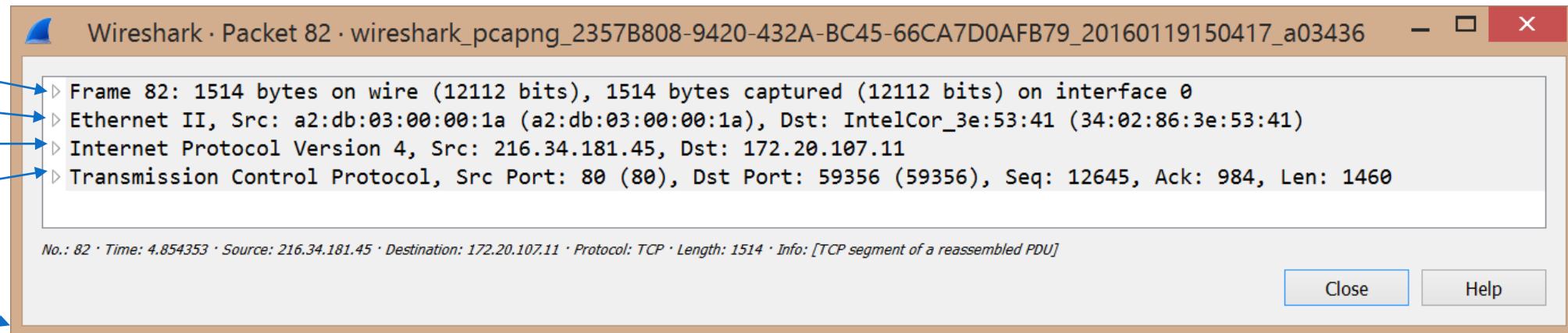- Levels 3, 2, and 1 add header (H) and tail (T) information to each packet

Information is added to the message as it travels down the OSI levels

	M					
	M					
	M					
	M					
H3	M	T3				
H2	H3	M	T3	T2		
H1	H2	H3	M	T3	T2	T1

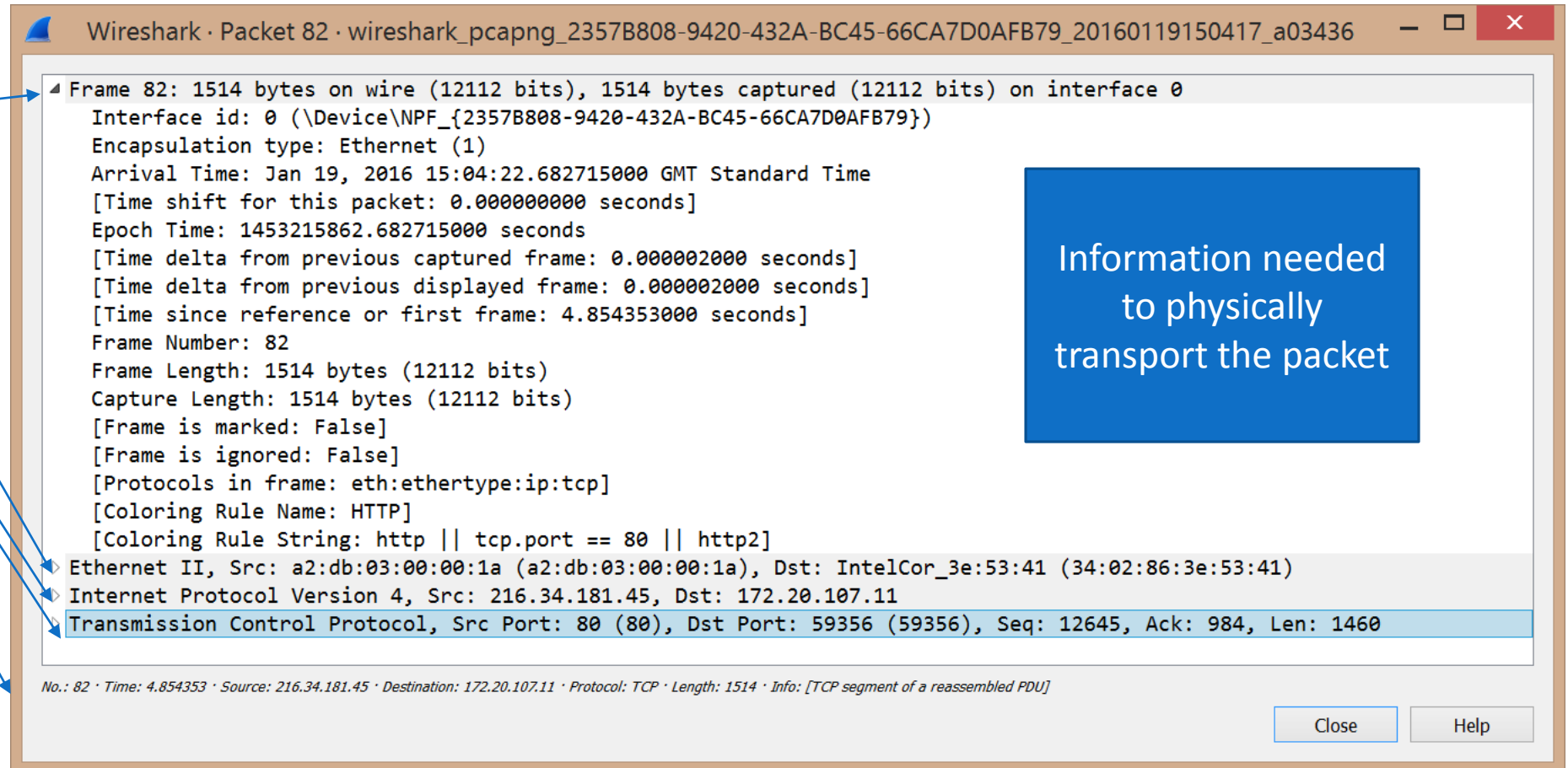| 7	**Application** Network process to application
6	**Presentation** Data representation and encryption
5	**Session** Interhost communication
4	**Transport** End-to-end connection and reliability
3	**Network** Path determination and IP (Logical Addressing)
2	**Data Link** MAC and LLC (Physical Addressing)
1	**Physical** Media, signal, and binary transmission

Header data on a packet

1. Physical
2. Data link
3. Network
4. Transport

...

7. Application

Wireshark · Packet 82 · wireshark_pcapng_2357B808-9420-432A-BC45-66CA7D0AFB79_20160119150417_a03436

▷ Frame 82: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits) on interface 0
▷ Ethernet II, Src: a2:db:03:00:00:1a (a2:db:03:00:00:1a), Dst: IntelCor_3e:53:41 (34:02:86:3e:53:41)
▷ Internet Protocol Version 4, Src: 216.34.181.45, Dst: 172.20.107.11
▷ Transmission Control Protocol, Src Port: 80 (80), Dst Port: 59356 (59356), Seq: 12645, Ack: 984, Len: 1460

No.: 82 · Time: 4.854353 · Source: 216.34.181.45 · Destination: 172.20.107.11 · Protocol: TCP · Length: 1514 · Info: [TCP segment of a reassembled PDU]

Close   Help

Frame header data on a packet

1. Physical
2. Data link
3. Network
4. Transport
…
7. Application

Wireshark · Packet 82 · wireshark_pcapng_2357B808-9420-432A-BC45-66CA7D0AFB79_20160119150417_a03436

```
▲ Frame 82: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits) on interface 0
      Interface id: 0 (\Device\NPF_{2357B808-9420-432A-BC45-66CA7D0AFB79})
      Encapsulation type: Ethernet (1)
      Arrival Time: Jan 19, 2016 15:04:22.682715000 GMT Standard Time
      [Time shift for this packet: 0.000000000 seconds]
      Epoch Time: 1453215862.682715000 seconds
      [Time delta from previous captured frame: 0.000002000 seconds]
      [Time delta from previous displayed frame: 0.000002000 seconds]
      [Time since reference or first frame: 4.854353000 seconds]
      Frame Number: 82
      Frame Length: 1514 bytes (12112 bits)
      Capture Length: 1514 bytes (12112 bits)
      [Frame is marked: False]
      [Frame is ignored: False]
      [Protocols in frame: eth:ethertype:ip:tcp]
      [Coloring Rule Name: HTTP]
      [Coloring Rule String: http || tcp.port == 80 || http2]
  ▷ Ethernet II, Src: a2:db:03:00:00:1a (a2:db:03:00:00:1a), Dst: IntelCor_3e:53:41 (34:02:86:3e:53:41)
  ▷ Internet Protocol Version 4, Src: 216.34.181.45, Dst: 172.20.107.11
  ▷ Transmission Control Protocol, Src Port: 80 (80), Dst Port: 59356 (59356), Seq: 12645, Ack: 984, Len: 1460
```

No.: 82 · Time: 4.854353 · Source: 216.34.181.45 · Destination: 172.20.107.11 · Protocol: TCP · Length: 1514 · Info: [TCP segment of a reassembled PDU]

Close   Help

Information needed to physically transport the packet

IP header data on a packet

1. Physical
2. Data link
3. Network
4. Transport
…
7. Application

Wireshark · Packet 82 · wireshark_pcapng_2357B808-9420-432A-BC45-66CA7D0AFB79_20160119150417_a03436

```
▷ Frame 82: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits) on interface 0
▷ Ethernet II, Src: a2:db:03:00:00:1a (a2:db:03:00:00:1a), Dst: IntelCor_3e:53:41 (34:02:86:3e:53:41)
▲ Internet Protocol Version 4, Src: 216.34.181.45, Dst: 172.20.107.11
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes
  ▷ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 1500
    Identification: 0xf76f (63343)
  ▷ Flags: 0x02 (Don't Fragment)
    Fragment offset: 0
    Time to live: 243
    Protocol: TCP (6)
  ▷ Header checksum: 0xe63b [validation disabled]
    Source: 216.34.181.45
    Destination: 172.20.107.11
    [Source GeoIP: Unknown]
    [Destination GeoIP: Unknown]
▷ Transmission Control Protocol, Src Port: 80 (80), Dst Port: 59356 (59356), Seq: 12645, Ack: 984, Len: 1460
```

No.: 82 · Time: 4.854353 · Source: 216.34.181.45 · Destination: 172.20.107.11 · Protocol: TCP · Length: 1514 · Info: [TCP segment of a reassembled PDU]

Close   Help

Version 4

Internet Protocol (IP) information

Type of the next header

Source and destination IP addresses

- Levels 7 and 6 involve the internal representation of the message
- Levels 5 and 4 involve setting up the connection
- Levels 3, 2, and 1 add header (H) and tail (T) information to each packet

Information is added to the message as it travels down the OSI levels

M

M

M

M

| H3 | M | T3 |

| H2 | H3 | M | T3 | T2 |

| H1 | H2 | H3 | M | T3 | T2 | T1 |
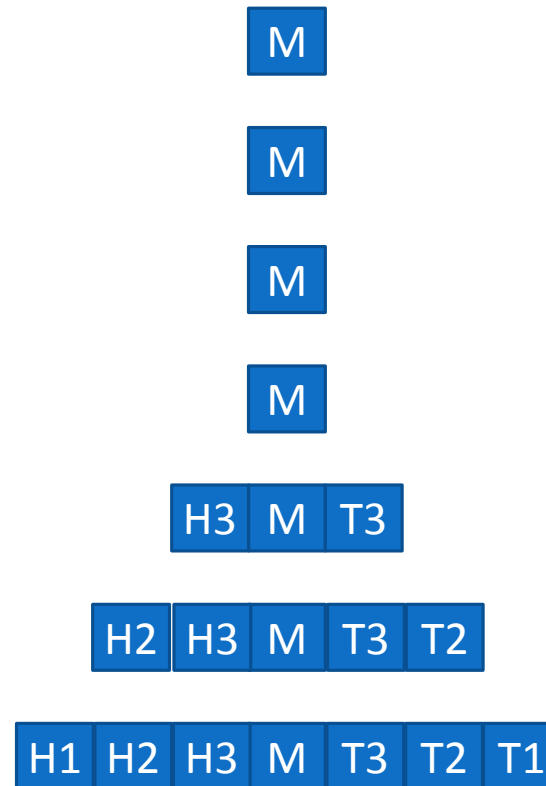
7	**Application** Network process to application
6	**Presentation** Data representation and encryption
5	**Session** Interhost communication
4	**Transport** End-to-end connection and reliability
3	**Network** Path determination and IP (Logical Addressing)
2	**Data Link** MAC and LLC (Physical Addressing)
1	**Physical** Media, signal, and binary transmission

This is me visiting
https://slashdot.org

- 6 packets were sent from my computer to the server

- 50 packets were sent from the server to my computer

This is me visiting http://vaniea.com

- Note the lack of https

- Why does the text look garbled anyway?

Firewalls

Firewalls

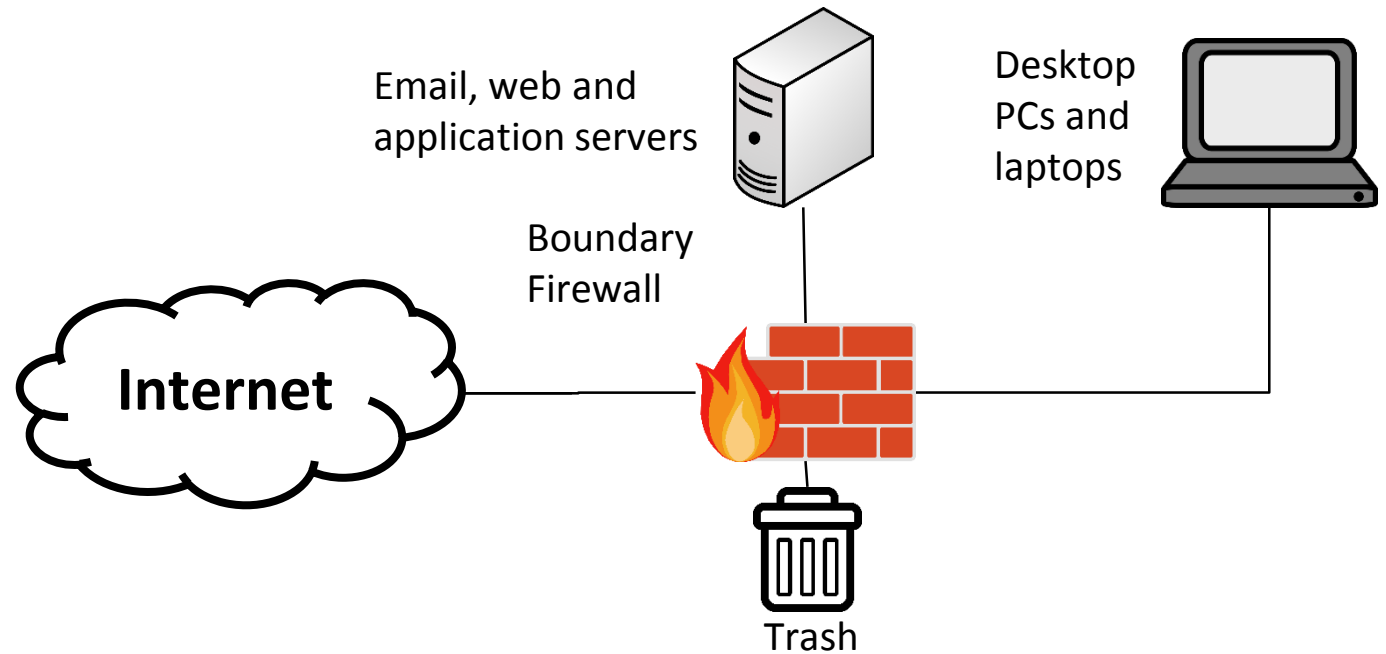- Firewalls divide the untrusted outside of a network from the more trusted interior of a network

- Often they run on dedicated devices

  ◦ Less possibilities for compromise – no compilers, linkers, loaders, debuggers, programming libraries, or other tools an attacker might use to escalate their attack

  ◦ Easier to maintain few accounts

  ◦ Physically divide the inside from outside of a network

Sample Network
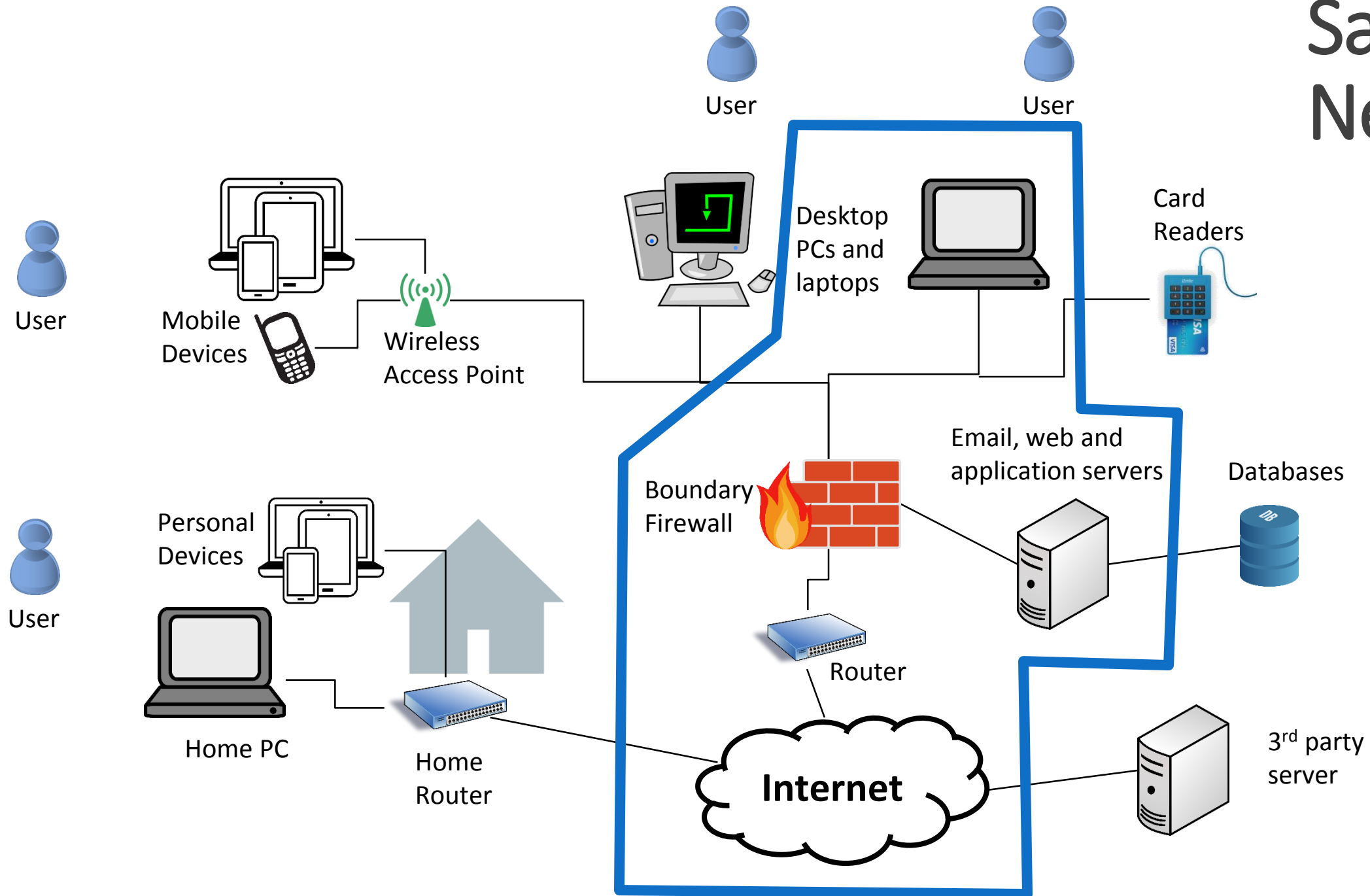
- Questionable things come from the internet AND from the local network

- Firewall applies a set of rules

- Based on rules, it allows or denies the traffic

- Firewalls can also act a routers deciding where to send traffic

Email, web and application servers

Desktop PCs and laptops

Boundary Firewall

Internet

Trash

Rule	Type	Source Address	Destination Address	Destination Port	Action
1	TCP	*	192.168.1.*	22	Permit
2	UDP	*	192.1681.*	69	Permit
3	TCP	192.168.1.*	*	80	Permit
4	TCP	*	192.168.1.18	80	Permit
5	UDP	*	192.168.1.*	*	Deny

Sender:
Apache server

Recipient:
Firefox user

#	Layer	Description
7	Application	Network process to application
6	Presentation	Data representation and encryption
5	Session	Interhost communication
4	Transport	End-to-end connection and reliability
3	Network	Path determination and IP (Logical Addressing)
2	Data Link	MAC and LLC (Physical Addressing)
1	Physical	Media, signal, and binary transmission

#	Layer	Description
7	Application	Network process to application
6	Presentation	Data representation and encryption
5	Session	Interhost communication
4	Transport	End-to-end connection and reliability
3	Network	Path determination and IP (Logical Addressing)
2	Data Link	MAC and LLC (Physical Addressing)
1	Physical	Media, signal, and binary transmission

Sender:
Apache server

7	**Application** Network process to application
6	**Presentation** Data representation and encryption
5	**Session** Interhost communication
4	**Transport** End-to-end connection and reliability
3	**Network** Path determination and IP (Logical Addressing)
2	**Data Link** MAC and LLC (Physical Addressing)
1	**Physical** Media, signal, and binary transmission

A firewall takes in network traffic and compares it to a set of rules. In order to do so it must first process several OSI levels to reach the data it needs.

For example, to filter out all traffic from IP 216.34.181.45 the packet needs to be processed through level 3 where IP addresses can be read.

Firewall

3	**Network** Path determination and IP (Logical Addressing)
2	**Data Link** MAC and LLC (Physical Addressing)
1	**Physical** Media, signal, and binary transmission

Recipient:
Firefox user

7	**Application** Network process to application
6	**Presentation** Data representation and encryption
5	**Session** Interhost communication
4	**Transport** End-to-end connection and reliability
3	**Network** Path determination and IP (Logical Addressing)
2	**Data Link** MAC and LLC (Physical Addressing)
1	**Physical** Media, signal, and binary transmission

Firewall ruleset from a custom home router

- Taken from an ARSTechnica article


```
root@ars-router: ~

##### Service rules
# OpenVPN
-A INPUT -p udp -m udp --dport 1194 -j ACCEPT

# ssh - drop any IP that tries more than 10 connections per minute
-A INPUT -p tcp -m tcp --dport 22 -m state --state NEW -m recent --set --name DE
FAULT --mask 255.255.255.255 --rsource
-A INPUT -p tcp -m tcp --dport 22 -m state --state NEW -m recent --update --seco
nds 60 --hitcount 11 --name DEFAULT --mask 255.255.255.255 --rsource -j LOGDROP
-A INPUT -p tcp -m tcp --dport 22 -j ACCEPT

# www - accept from LAN
-A INPUT -i p1p1 -p tcp -m tcp --dport 80 -j ACCEPT
-A INPUT -i p1p1 -p tcp -m tcp --dport 443 -j ACCEPT

# DNS - accept from LAN
-A INPUT -i p1p1 -p tcp --dport 53 -j ACCEPT
-A INPUT -i p1p1 -p udp --dport 53 -j ACCEPT

# default drop because I'm awesome
-A INPUT -j DROP

##### forwarding ruleset
```

Image: http://arstechnica.co.uk/gadgets/2016/01/numbers-dont-lie-its-time-to-build-your-own-router/

There are many types of Firewalls

Key differences include:

- How implemented
  - Software – slower, easier to deploy on personal computers
  - Hardware – faster, somewhat safer, harder to add in
- Number of OSI levels of processing required
  - Packet size (level 1)
  - MAC (level 2) and IP (level 3) filtering
  - Port filtering (level 3)
  - Deep packet (level 4+)

Today we will talk about:

- Packet filtering gateway
- Stateful inspection firewall
- Application proxy
- Personal firewalls

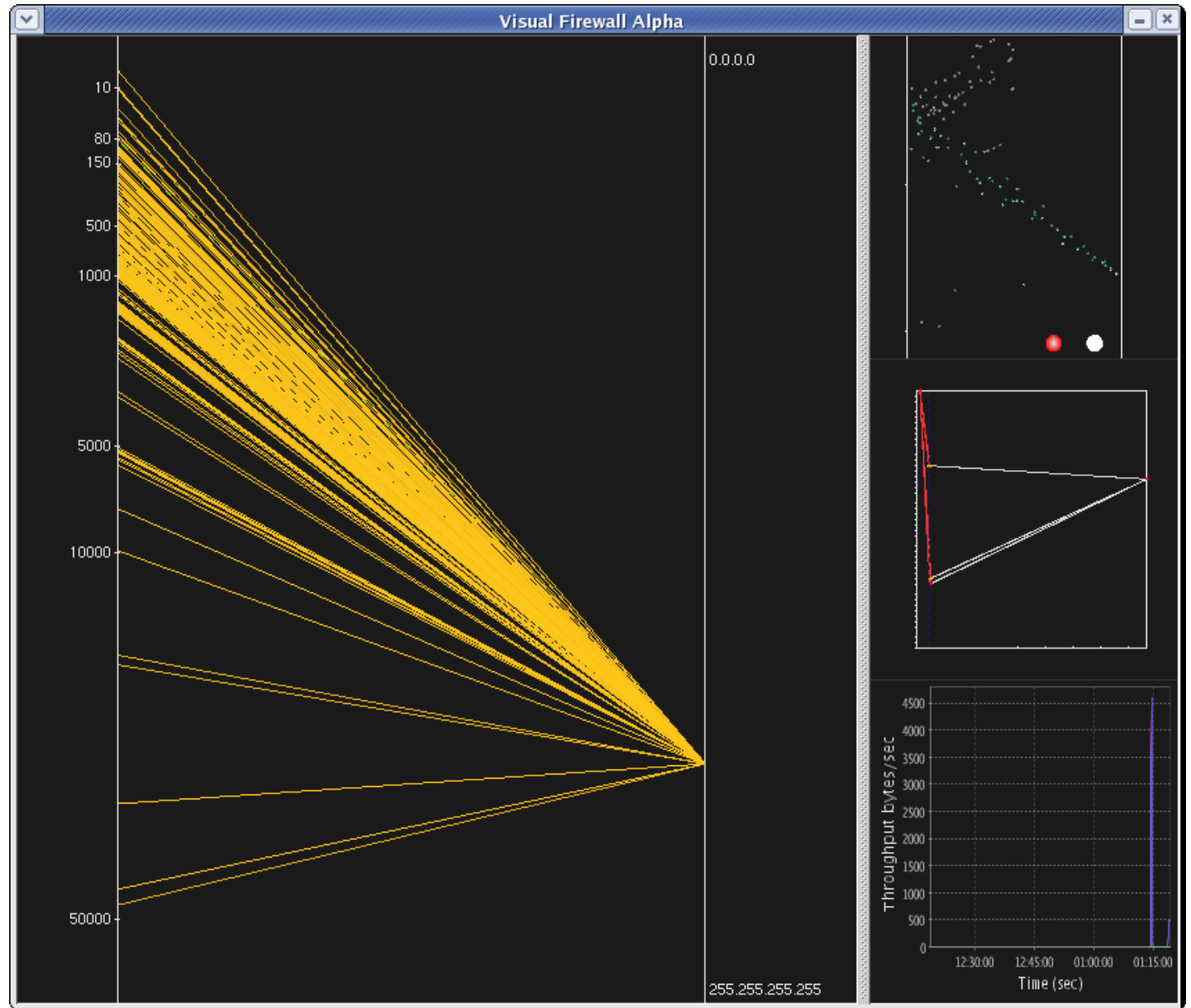# Packet filtering gateway or screening router

- Simplest – compares information found in the headers to the policy rules

- Operate at OSI level 3

- Source addresses and ports can be forged, which a packet filter cannot detect

- Design is simple, but tons of rules are needed, so it is challenging to maintain

Stateful inspection firewall

- Maintains state from one packet to another

- Similar to a packet filtering gateway, but can remember recent events

- For example, if a outside host starts sending packets to many internal destination ports (aka a port scan) a stateful firewall would record the number of ports probed and once it is over the threshold specified in the policy it would block all further traffic
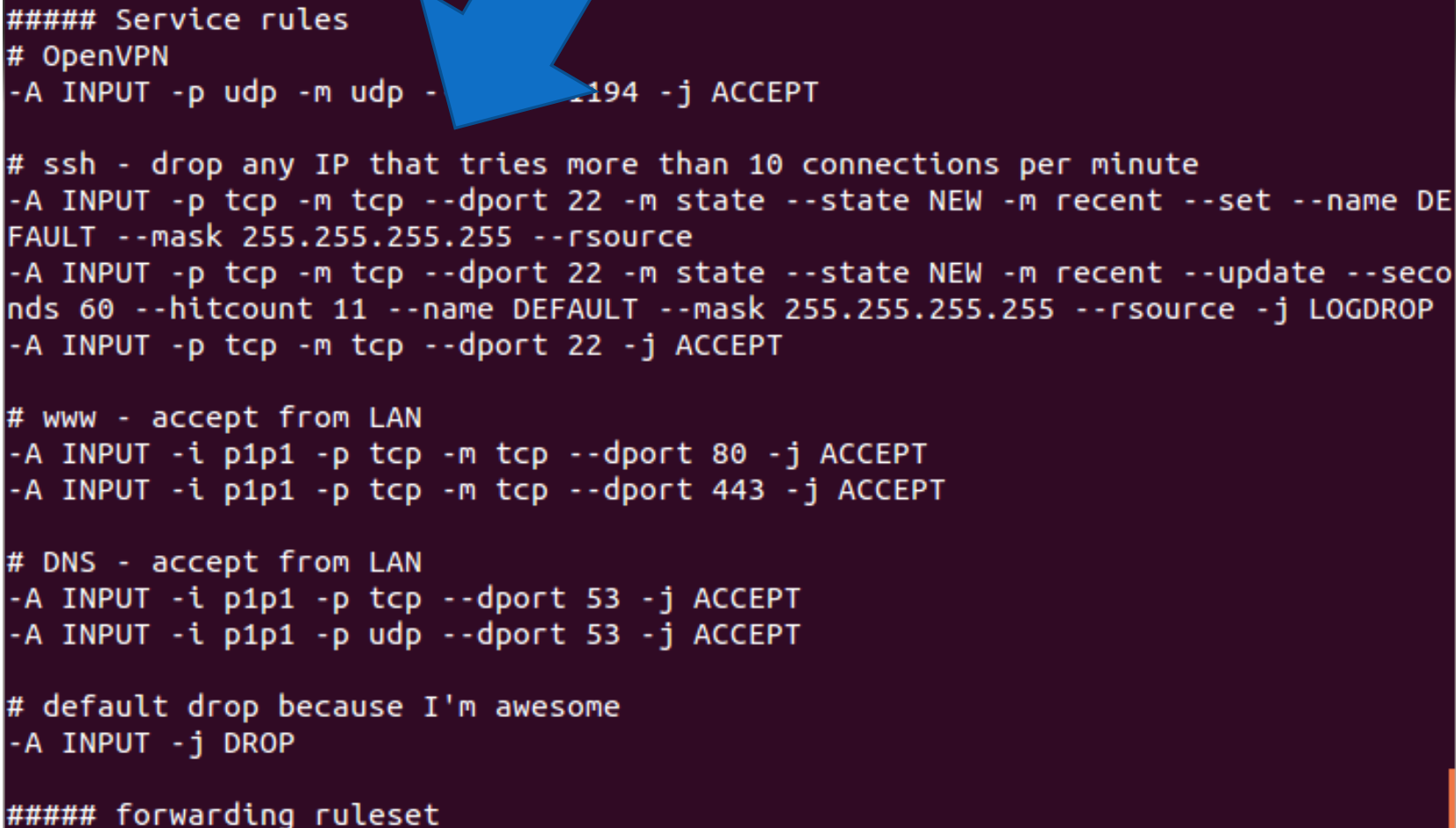
Port scan

- An attacker is looking for applications listening on ports

- A single IP address (right) is contacting many ports (left) to see if any respond

Image: http://chrislee.dhs.org/projects/visualfirewall.html

Firewall ruleset from a custom home router

- Taken from an ARSTechnica article


```
root@ars-router: ~

##### Service rules
# OpenVPN
-A INPUT -p udp -m udp -        :194 -j ACCEPT

# ssh - drop any IP that tries more than 10 connections per minute
-A INPUT -p tcp -m tcp --dport 22 -m state --state NEW -m recent --set --name DE
FAULT --mask 255.255.255.255 --rsource
-A INPUT -p tcp -m tcp --dport 22 -m state --state NEW -m recent --update --seco
nds 60 --hitcount 11 --name DEFAULT --mask 255.255.255.255 --rsource -j LOGDROP
-A INPUT -p tcp -m tcp --dport 22 -j ACCEPT

# www - accept from LAN
-A INPUT -i p1p1 -p tcp -m tcp --dport 80 -j ACCEPT
-A INPUT -i p1p1 -p tcp -m tcp --dport 443 -j ACCEPT

# DNS - accept from LAN
-A INPUT -i p1p1 -p tcp --dport 53 -j ACCEPT
-A INPUT -i p1p1 -p udp --dport 53 -j ACCEPT

# default drop because I'm awesome
-A INPUT -j DROP

##### forwarding ruleset
```

Image: http://arstechnica.co.uk/gadgets/2016/01/numbers-dont-lie-its-time-to-build-your-own-router/

Application proxy

- Simulates the (proper) effects of an application at OSI level 7
- Effectively a protective Man In The Middle that screens information at an application layer (OSI 7)
- Allows an administrator to block certain application requests.
- For example:
  - Block all web traffic containing certain words
  - Remove all macros from Microsoft Word files in email
  - Prevent anything that looks like a credit card number from leaving a database

Personal firewalls

- Runs on the workstation that it protects (software)
- Provides basic protection, especially for home or mobile devices
- Malicious software can disable part or all of the firewall
- Any rootkit type software can disable the firewall

Think-pair-share

Imagine you want to put a firewall in front of the email server

- Why is deep packet inspection easier to do on email than on normal network traffic?

- As a malicious actor, how might I go around your email firewall?

Intrusion Detection Systems (IDS)

Firewalls are preventative, IDS detects a potential incident in progress

- At some point you have to let some traffic into and out of your network (otherwise users get upset)

- Most security incidents are caused by a user letting something into the network that is malicious, or by being an insider threat themselves

- These cannot be prevented or anticipated in advance

- The next step is to identify that something bad is happening quickly so you can address it

Signature based

- Perform simple pattern matching and report situations that match the pattern

- Requires that admin anticipate attack patterns in advance

- Attacker may test attack on common signatures

- Impossible to detect a new type of attack

- High accuracy, low false positives

Heuristic based

- Dynamically build a model of acceptable or "normal" behavior and flag anything that does not match

- Admin does not need to anticipate potential attacks

- System needs time to warm up to new behavior

- Can detect new types of attacks

- Higher false positives, lower accuracy

Number of alarms is a big problem

- In the Target breach the IDS did correctly identify that there was an attack on the Target network

- There were too many alarms going off to investigate all of them in great depth

- Some cyberattack insurance policies state that if you know about an attack and do nothing they will not cover the attack.

- Having a noisy IDS can potentially be a liability

Network Address Translation (NAT)

IPv4

- Version 4 of the Internet Protocol
  - 192.168.2.6
- There are less than 4.3 billion IPv4 addresses available
- We do not have enough addresses for every device on the planet
- Answer: Network Address Translation
  - Internal IP different than external IP
  - Border router maps between its own IP and the internal ones

Questions