Check Point®
SOFTWARE TECHNOLOGIES LTD.

Workshop in Information Security

Building a Firewall within the Linux Kernel

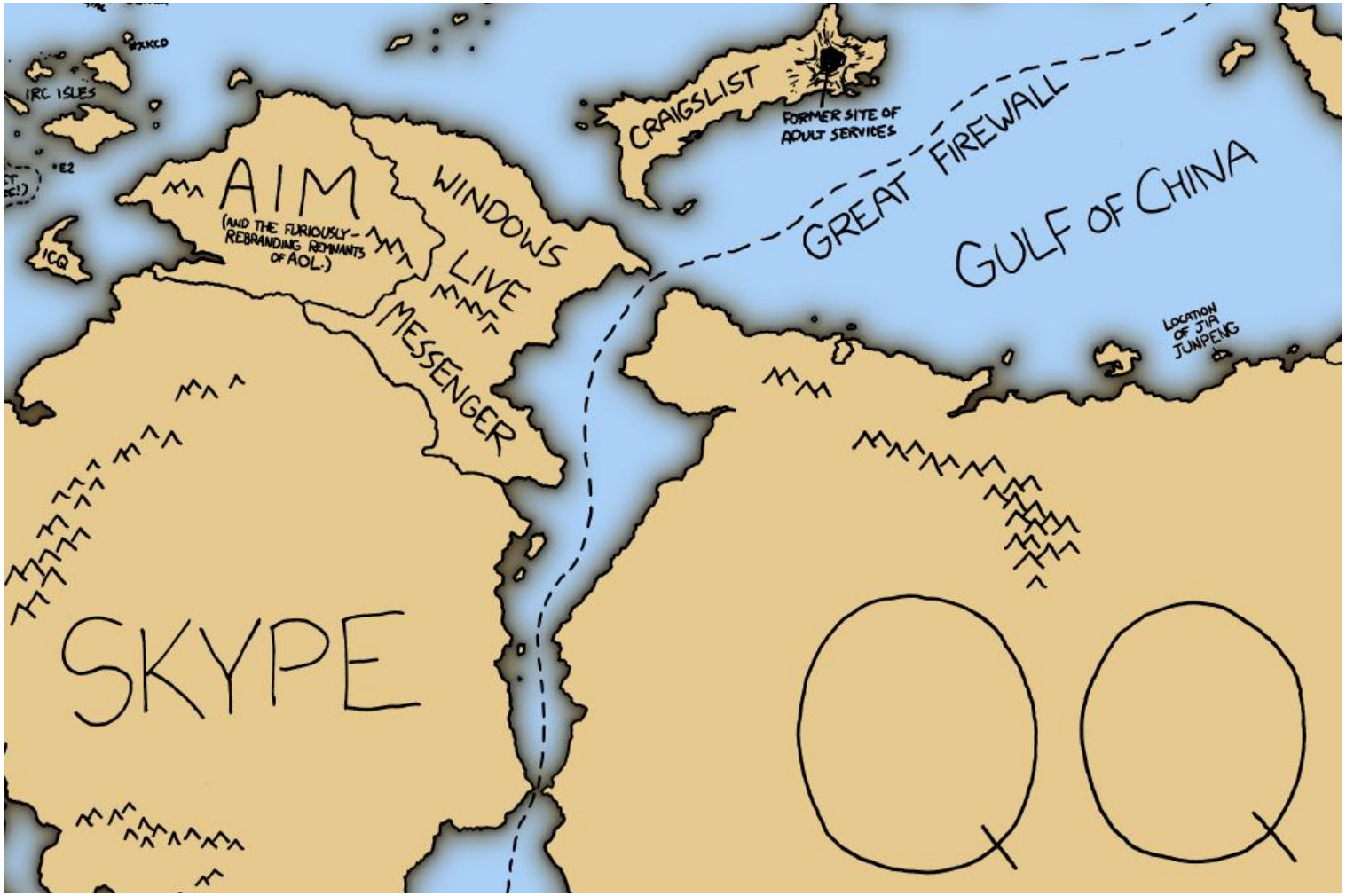
Intro to firewalls

Lecturer: Eran Tromer

Teaching assistant: Ariel Haviv

Advisor: Assaf Harel

Online Communities 2 3d.xkcd.com/802



Low Level Firewalls

1. Intro to Firewalls
2. Packet Filtering
3. Circuit Level

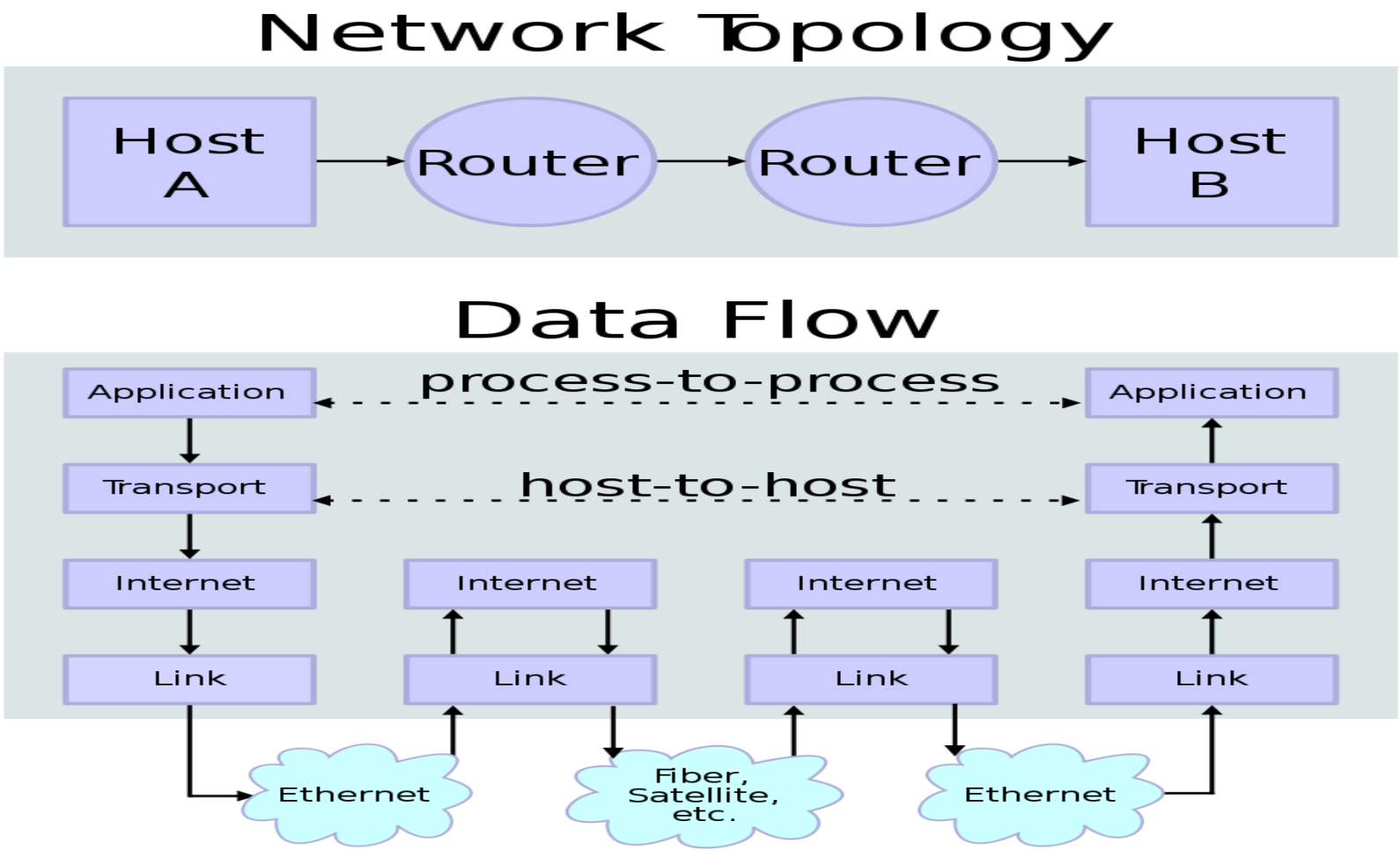
Low Level Firewalls

1. **Intro to Firewalls**
2. Packet Filtering
3. Circuit Level

Intro to Firewalls

- A piece of soft/hardware intended to keep a certain network secure:
  - Enforce protocol correctness.
  - Minimize chance of intrusion & attacks.
- Can operate in different levels of the OSI.
  - First firewalls looked up to the TCP/IP level.
  - Today's firewalls inspect all the way up to the application level.

Intro to Firewalls



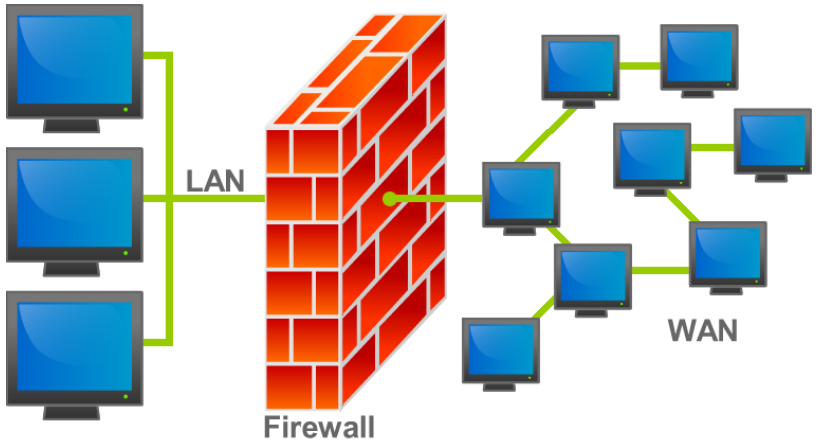
(Source: http://en.wikipedia.org/wiki/TCP/IP_model)

Intro to Firewalls

- A firewall needs to look into packets, so it must a have some communication with the kernel.
- Needs to decide fast, we want maximum throughput. Can't afford slowing down the traffic.
- Needs to be configurable, and smart.
- Needs to provide some way for the user to see what's going on inside.

Intro to Firewalls

- The purpose is to stand between the local network and the internet:



- Can be achieved by a physical appliance

- Or a software-based firewall.
  - As a kernel module on a running OS
  - As a dedicated virtual machine

Low Level Firewalls

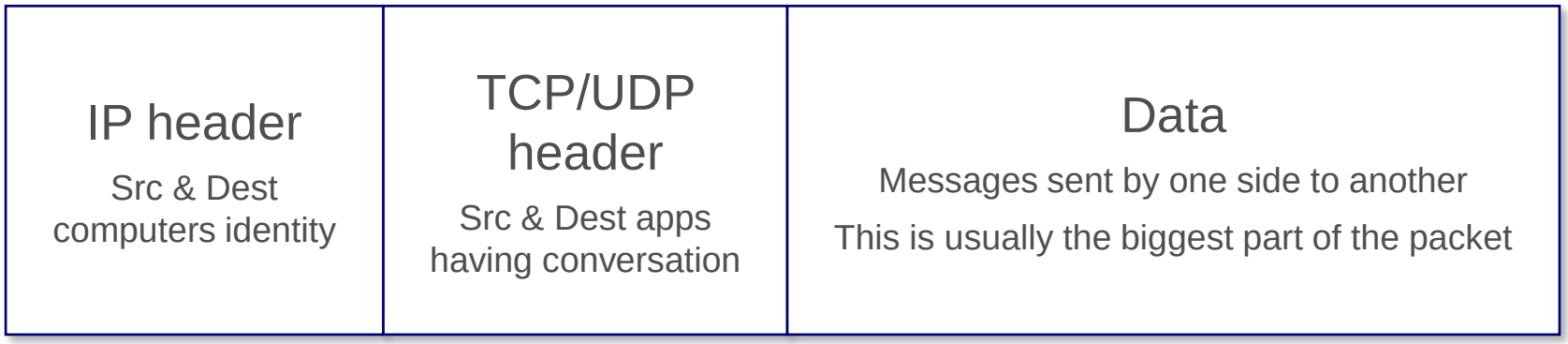
1. Intro to Firewalls
2. **Packet Filtering**
3. Circuit Level

Packet Filtering

- Actually, mainly connection filtering.
- A connection is:
  - Source ip and port.
  - Destination ip and port.
- We make certain connections legal, and the others illegal.
- For example, we allow incoming connections to the host 10.1.1.1 only on port 80.
- Another example – disallow all connections from 172.23.31.0/24 network.

Packet Filtering

- We look into the IP header of the packet to identify the source and destination IP, and into the UDP/TCP header to identify the source and destination ports.
- Here's a packet:



Low Level Firewalls

1. Intro to Firewalls
2. Packet Filtering
3. **Circuit Level**

Circuit Level

- A TCP connection is a conversation between two computers.
- We can keep the state of every TCP (but can be any stateful protocol) connection.
- TCP begins with a handshake, and ends with a FIN, RST or disappearance of one of the sides.
- The goals: Protocol enforcement & Network protection. We verify no out of state communication passes. Packets that don’t belong to any active conversation, don’t belong to the net the firewall is protecting.

Circuit Level

- We can keep track of who initiated the conversation, and what is its state at any given time, by looking into the packet's headers.
- Usually we give every connection an arbitrary timeout (even though there is no timeout in the RFC). Just to be able to delete old records and make room for new ones, if they are not ended 'by the book', or one of the sides just dies.