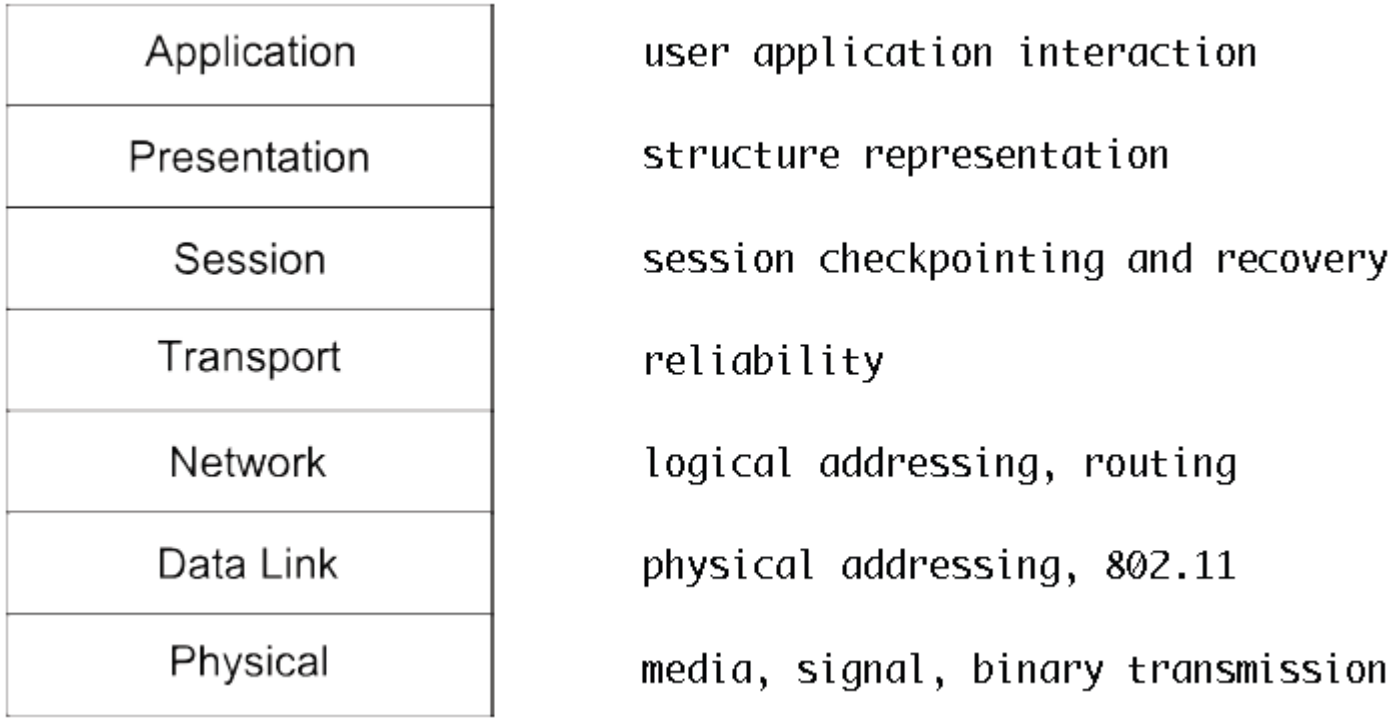
CS443 - Network Security

Note Title 1/30/2013

Announcements

- HW due Tuesday
- Lab 3 will be up today
  due 1 week from Tuesday

Networking Basics: The OSI Model



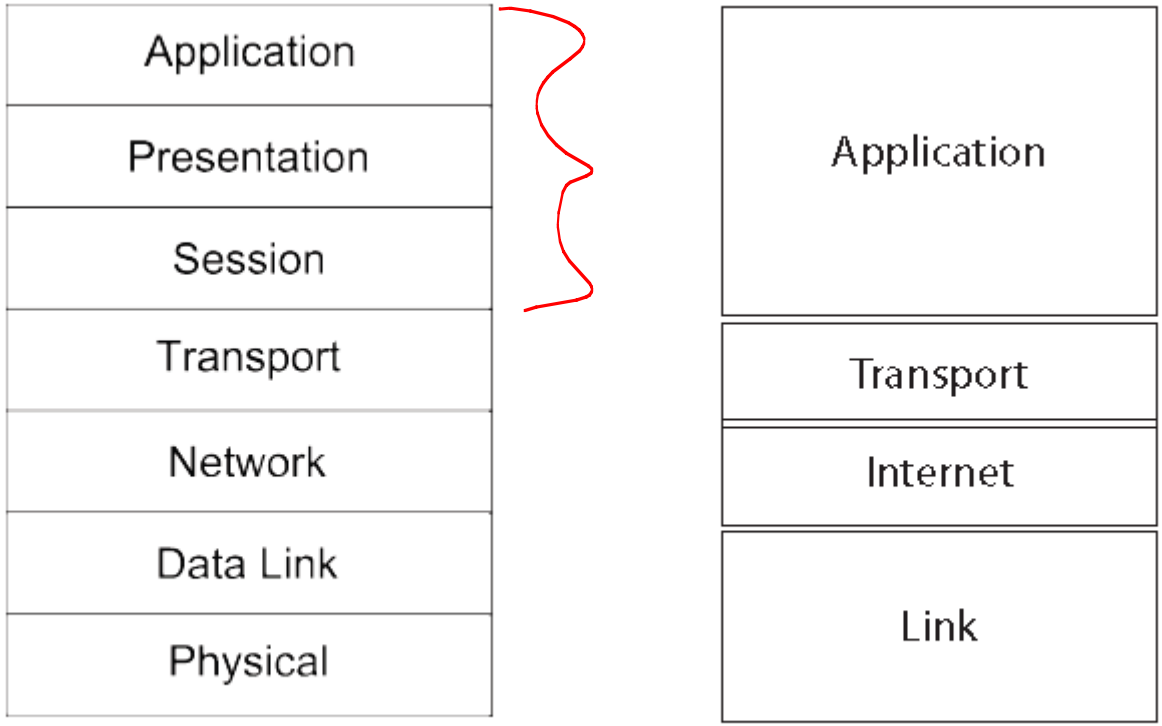
TCP/IP

There are different layers + implementations in OSI Model.

The internet protocol suite (TCP/IP) is an implementation of the OSI.

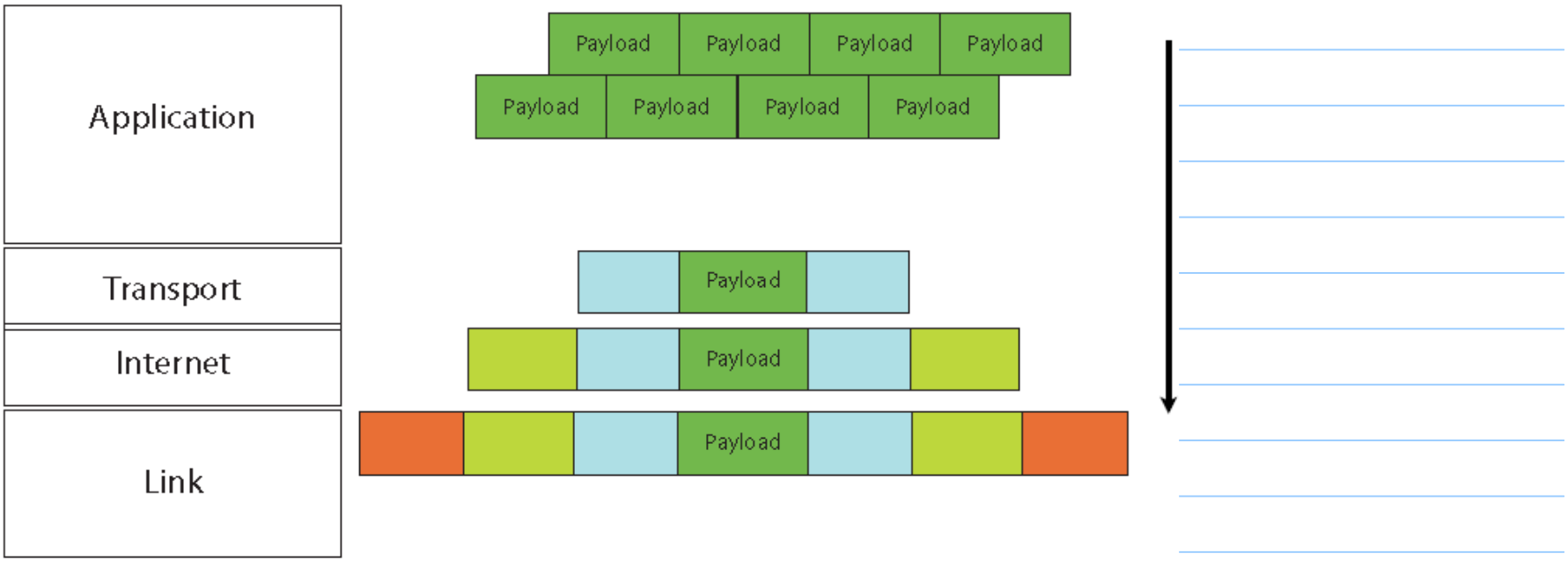
It doesn't use as fine of granularity, but it also has different "levels".

TCP/IP Layers



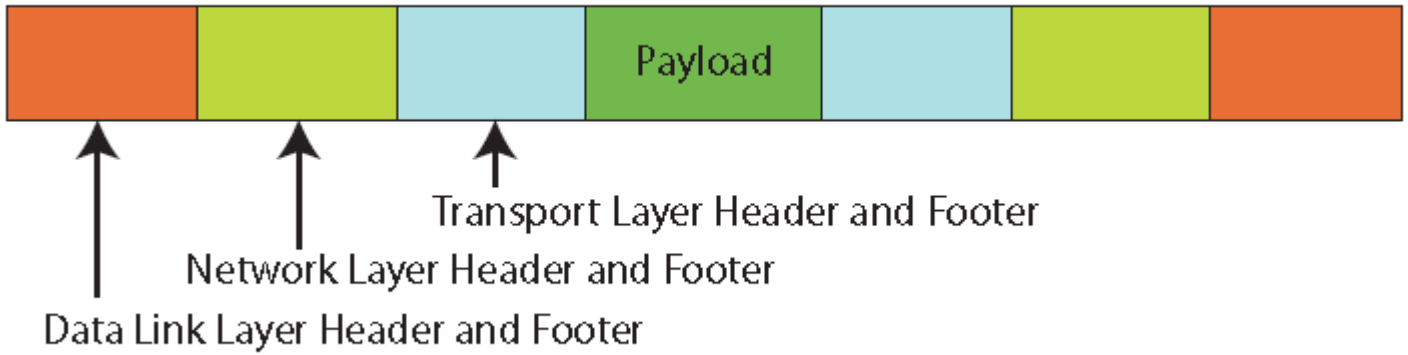
Transmitting Data:

Data is divided in packets, and each layer adds headers.



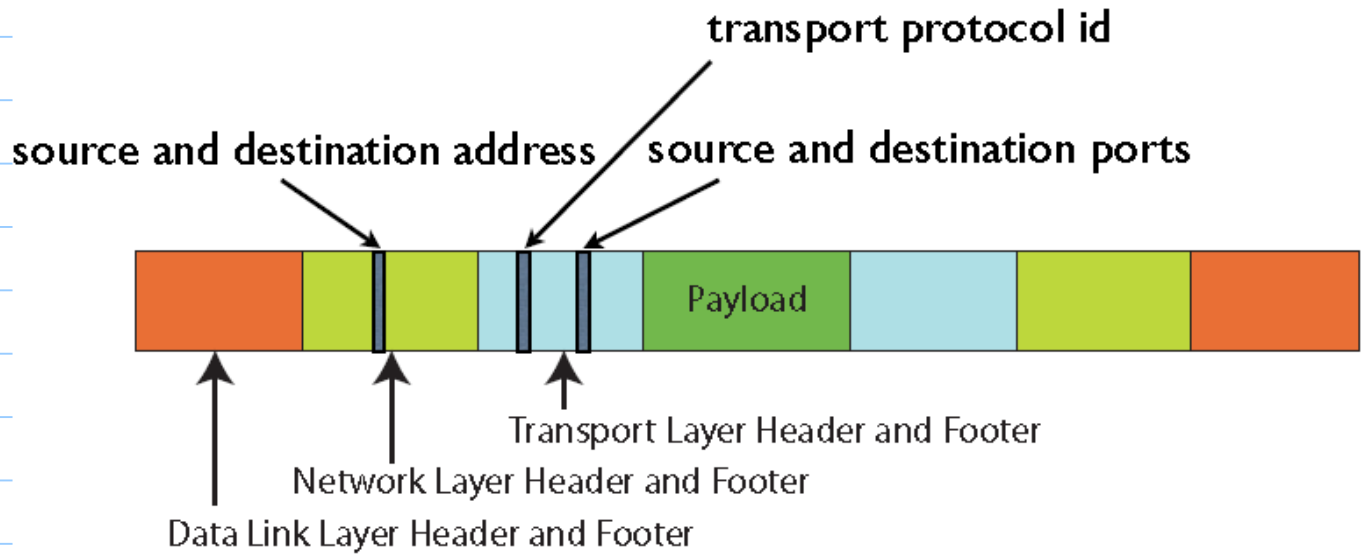
Security View

Certain areas of these headers & footers are very interesting from a security point of view.



In particular, much information which details possible vulnerabilities is available!

Note: This data can't really be hidden!



Relevant Data in Headers

- IP-address : 168.10.10.1
- MAC address : hard coded identifier
  8C:6F:...
- Port number : up to 1024 - restricted
  up to 64,000 - roving
- Protocol id : identifies a type of communication

Two major issues:

1. System protection:

   Machines must read packets, but info in them could be dangerous.

   - Firewalls

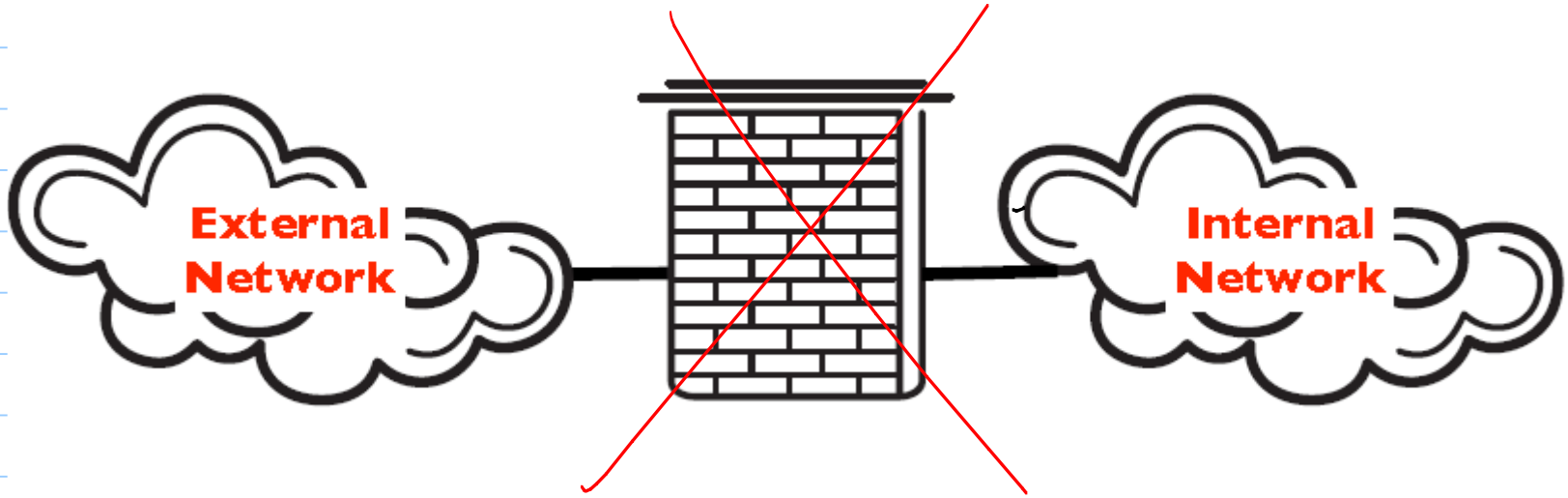
2. Hiding information:

   Nothing in IP prevents intermediaries from reading payloads of packets.

   - IPSec

Firewalls : System Protection

All traffic from the inside network to the outside (or vice versa) must pass through the firewall.



Different Systems

host based

- Firewalls can be dedicated systems, or pieces of local software.

personal

- Many different types, with different levels of safety depending of the amount of checking or monitoring.

(Generally, as always, faster means less secure.)

Packet Filtering Firewalls

Rules are based on the packet headers.

Sometimes called a "stateless firewall", since has no memory of previous connections or more complex monitoring.

Generally, packets are simply authorized based on source or destination IPs and ports, as well as particular protocol ids.

Proxies

A proxy computer is an intermediate agent or sever that acts between two endpoints without allowing direct communications.

Ex: HTTP proxy:

- takes webpage requests & sends them out
- cache results for later use
- improve speed & bandwidth

Proxy Firewalls - stateful

A proxy firewall bases access control on contents of packets as well as header info.

Advantages:
- much better at monitoring
- speed benifits - bandwidth

Disadvantages:
- large infrastructure
- speed (in terms of processing)

More on stateful firewalls

In general, TCP connections fix a port number for all communication.

(Higher number ports are reallocated as needed for these connections.)

Stateful firewalls track established TCP connections & only allow traffic to specific ports for duration of one connection.

Example: IPTables

A native Linux firewall tool providing stateful monitoring.

Can be run on an individual machine, or on a server to protect larger networks.

This tool will be the focus of the next lab.

Sample: interactive use:

```
$ iptables -t filter -A INPUT -m state --state NEW -p tcp -s 192.168.0.1 --dport 23 -j REJECT
```

`iptables`

We're going to use the iptables tool to insert a new rule into netfilter.

`-t filter`

This rule is going to go in the filter table, which is the built-in packet filtering table. This rule will apply only to:

`-A INPUT`

packets that have been put into the `INPUT` chain either by the kernel or by some previous rule and which:

`-m state --state NEW`

represent a new connection,

`-p tcp`

are Transmission Control Protocol (TCP) packets,

`-s 192.168.0.1`

are from the host 192.168.0.1,

`--dport 23`

and are destined for port 23.

`-j REJECT`

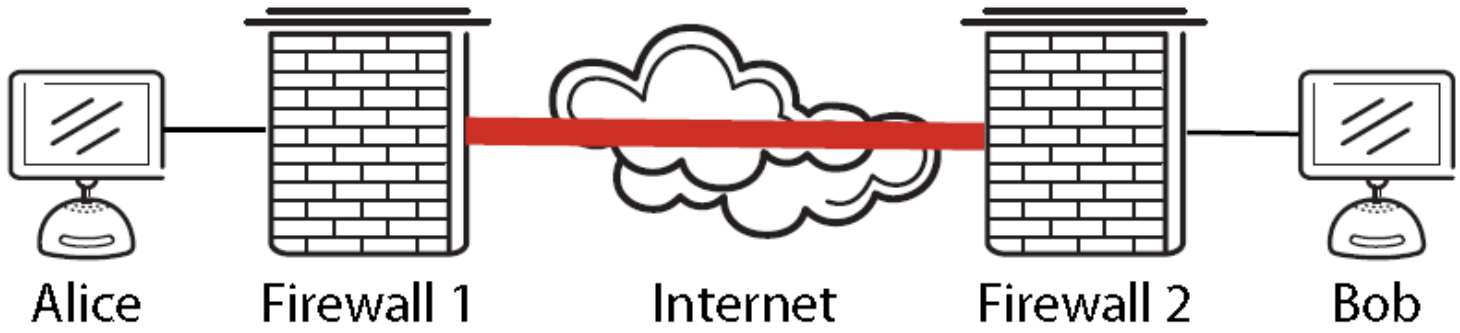
Reject any matching packet. Processing of all packets matching this rule will instantly jump to the built-in target REJECT, which means that the packet will be rejected by the kernel with some kind of network error message.

Notes on iptables:

- Can interact from command line, or (more commonly) edit the shell file controlling it.
- Requires root access!
- This is actually a user interface tool for administering netfilter functions in the Linux kernal.
- See assignment for full discussion and overviews. - reading assignment for Tuesday.

(2) IPSec : Hiding information

Data sent over a network is inherently insecure. IPSec is a protocol that adds encryption at a low layer of TCP/IP model.

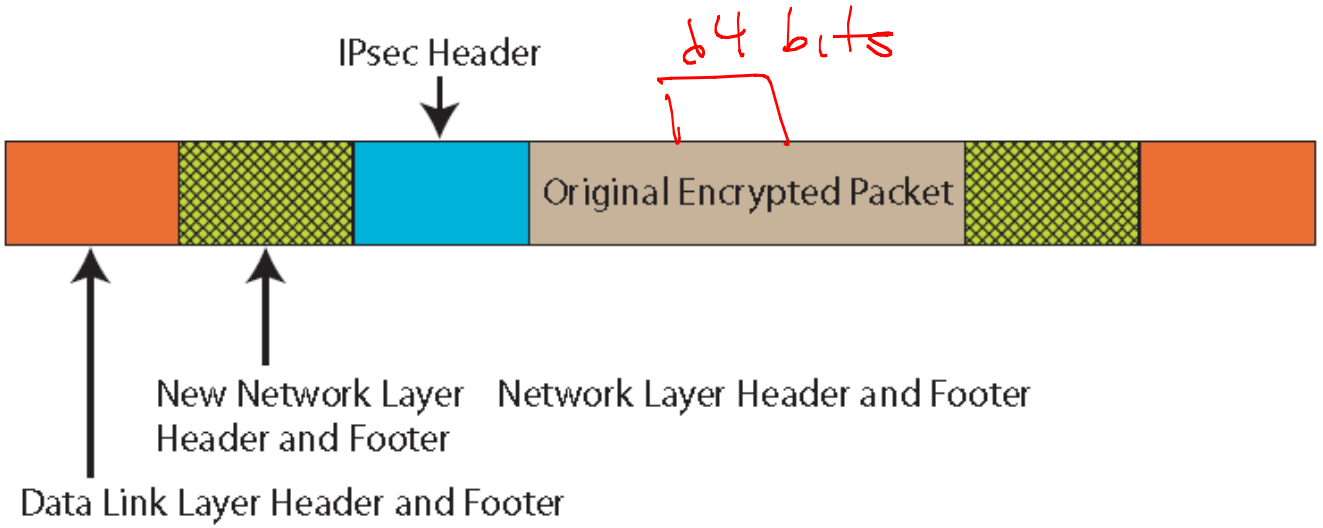


Modes

- In transport mode, only the packets are encrypted. However, authentication headers provide assurance that IP addressed can't be modified (since hash value is invalidated).

- In tunnel mode, the entire packet is encrypted, and new headers are created.
  (This is how VPNs are created.)

Tunnel Mode

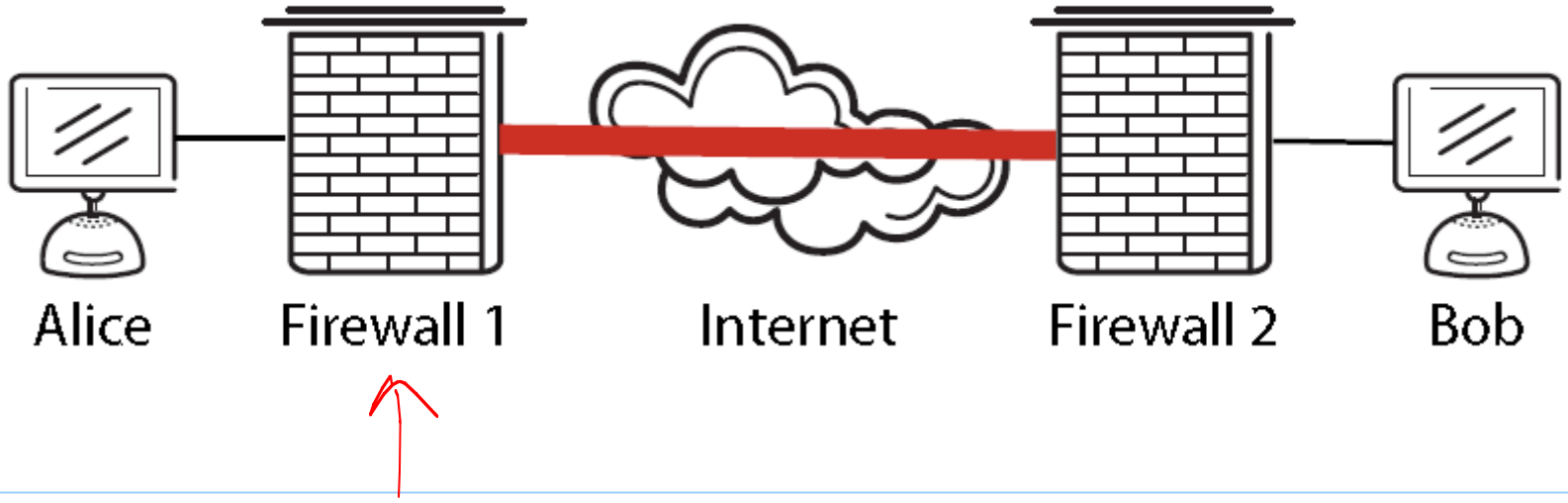


"Refers to keeping the original IP packet intact and adding a new IP header and IPsec information outside.

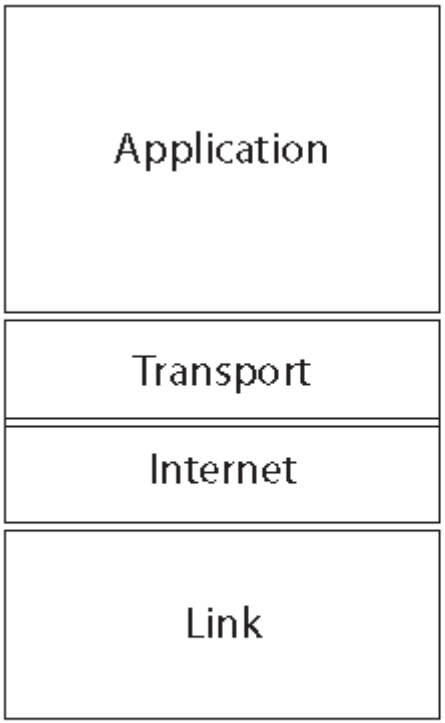
Content taken from "Network Security: Private Communication in a Public World."

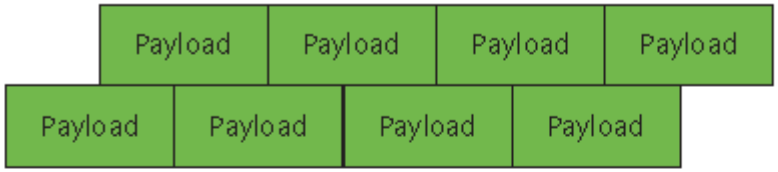
An example of tunnel mode:

Alice wants to send Bob a message.



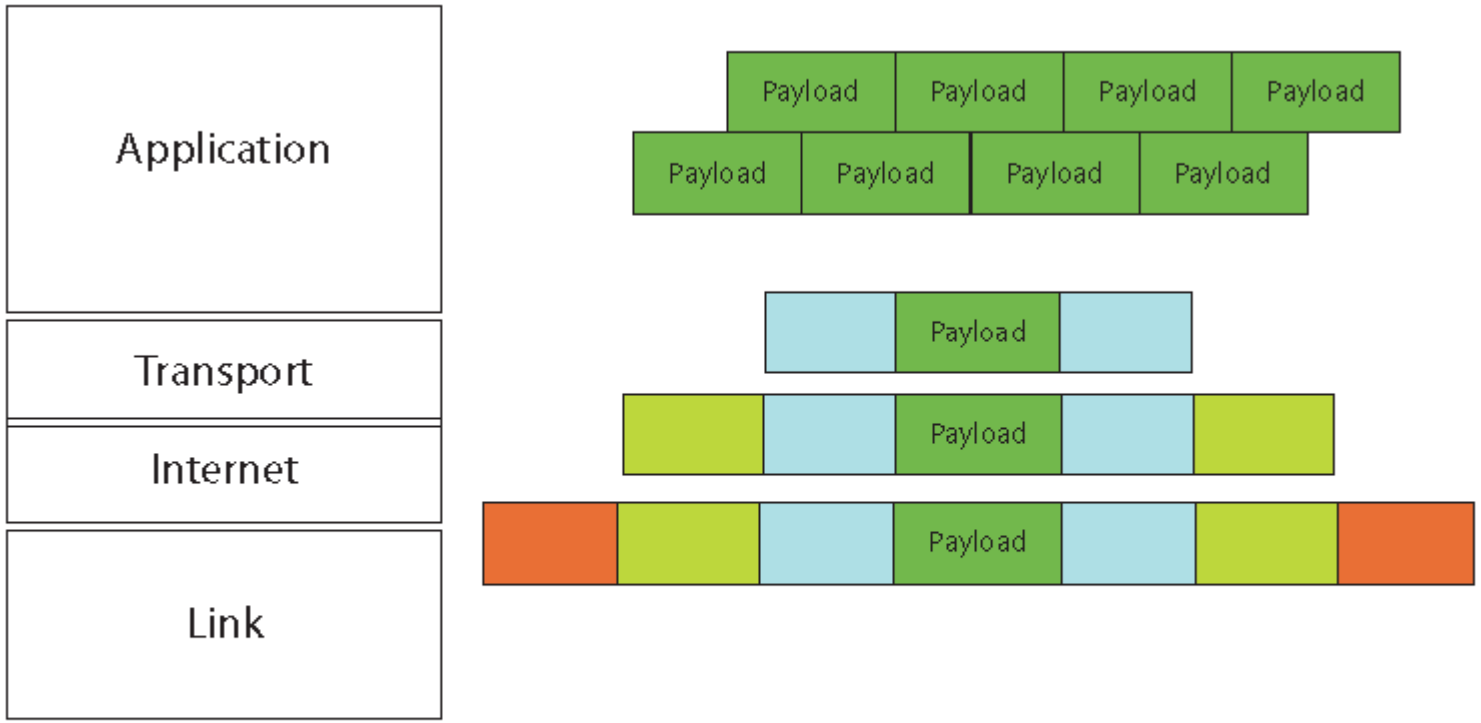
Step 1:





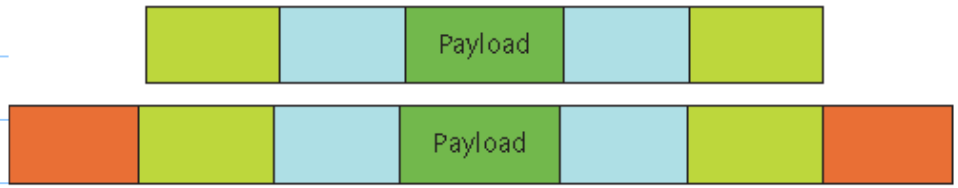
Alice sends an e-mail as usual.

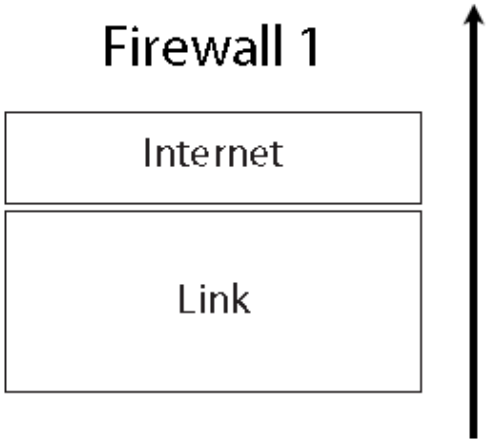
Step 2:



The e-mail is divided into packets. Headers are added at each layer.

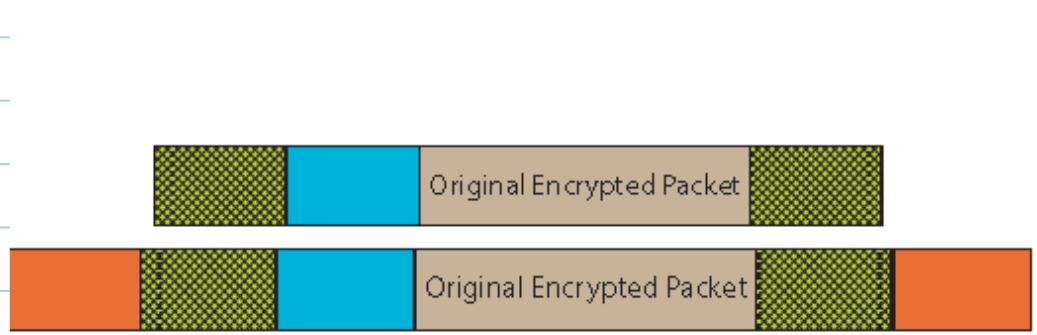
At the firewall:
(either internal or external)

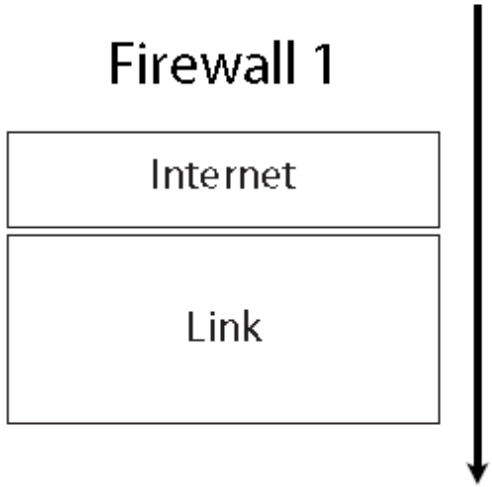




Each packet makes its way to Alice's firewall.

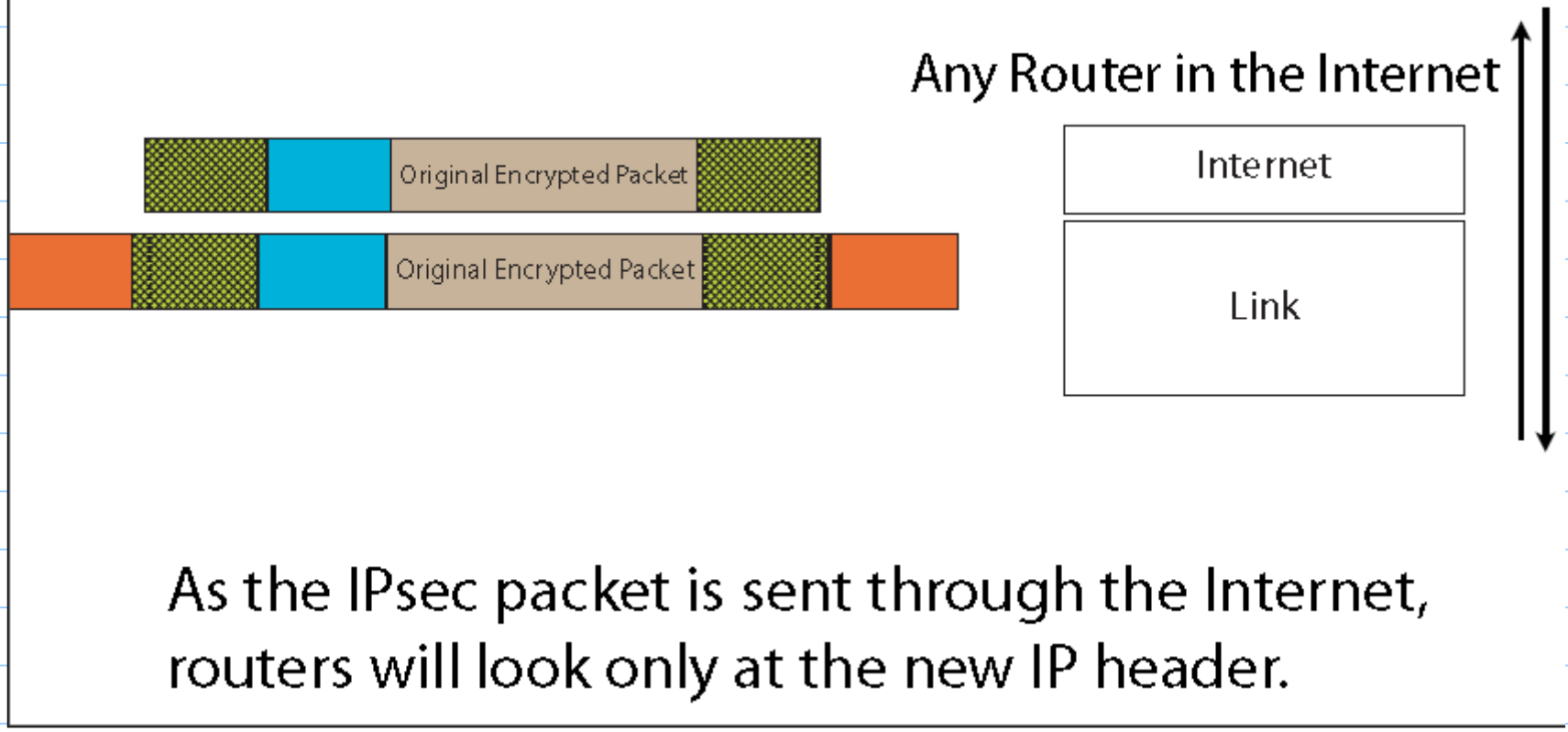
At the firewall (cont):





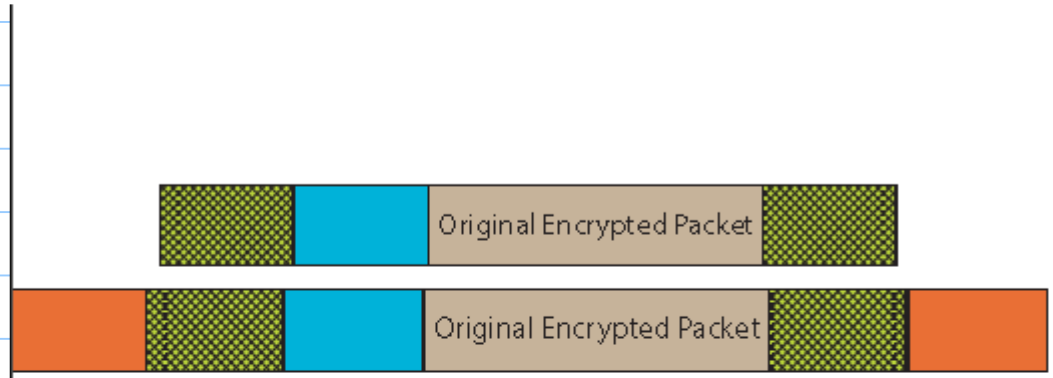
The IPsec-enabled firewall encrypts the packet, adds a IPsec header and adds a new IP header.

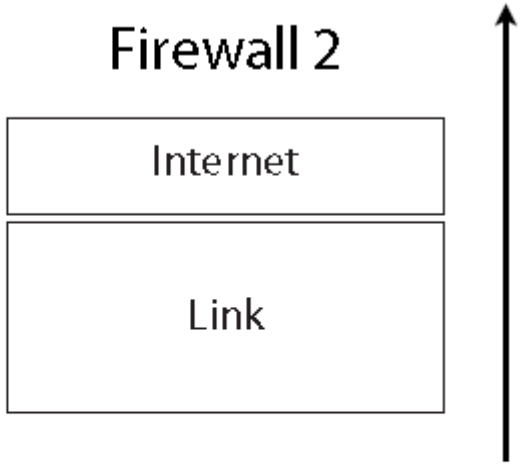
Intermediate Nodes



As the IPsec packet is sent through the Internet, routers will look only at the new IP header.

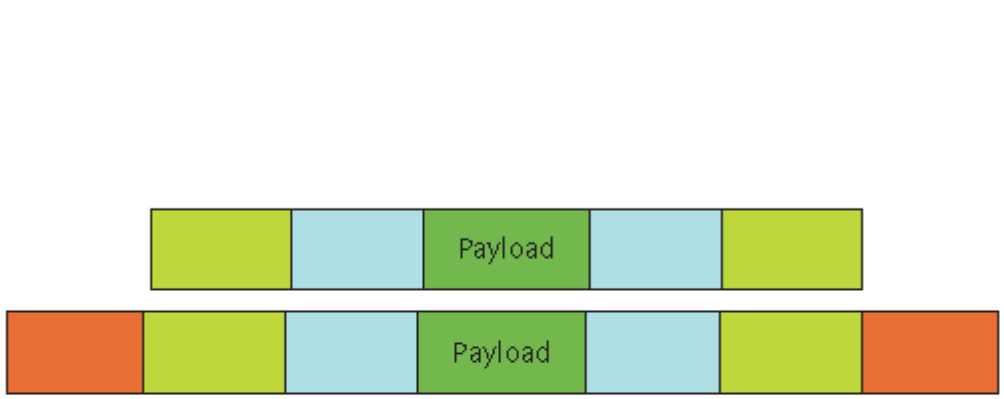
At the next firewall:

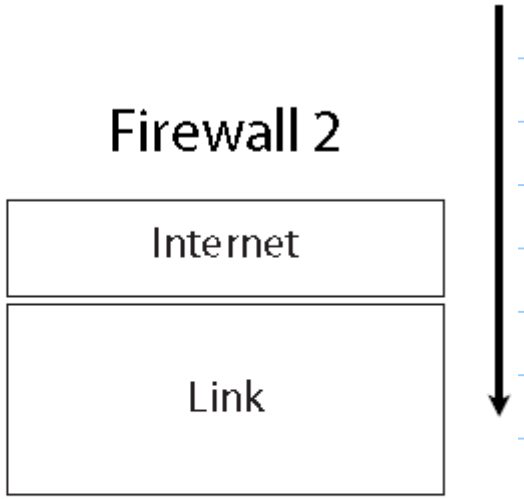




When the IPsec packet reaches Bob's firewall 2...

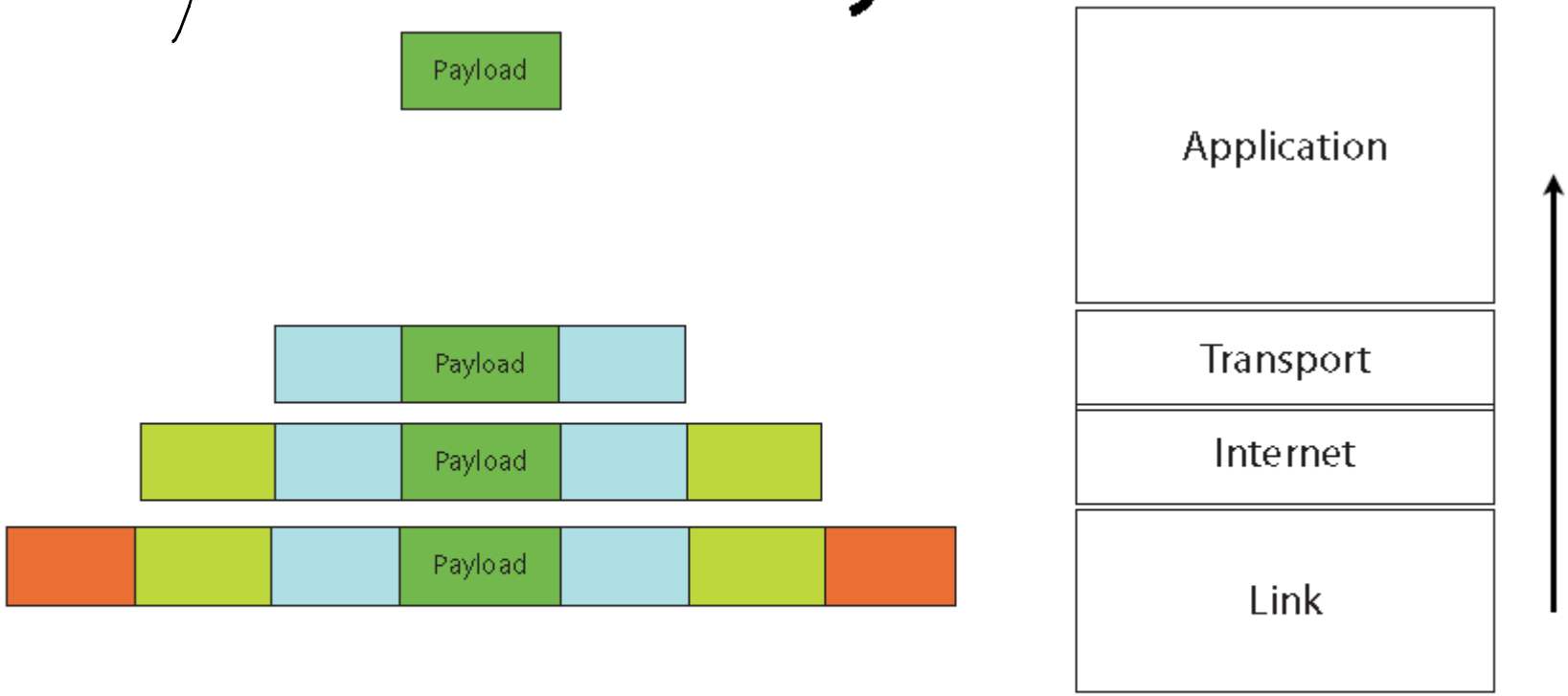
Firewall 2 resends:





Firewall 2 decrypts it, gets the original packet, and forwards it along to Bob.

Finally, at the destination:



At Bob's machine, all the headers are removed and the packets are assembled into Alice's e-mail.

Advantage of IPSec:

Encryption & security is at a low level.

So unlike a secure protocol (like SSH), this builds security on top of other protocols.

Provides authenticity, integrity, and confidentiality.

Next time:

Pick up more on network security

Details on iptables